UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENADORIA DO CURSO DE ENGENHARIA DE SOFTWARE

JÉSSICA IARA PEGORINI

AUTENTICIDADE, INTEGRIDADE E ANONIMIDADE NO SISTEMA DE VOTAÇÃO ELETRÔNICA DO BRASIL

TRABALHO DE CONCLUSÃO DE CURSO

DOIS VIZINHOS

2019

JÉSSICA IARA PEGORINI

AUTENTICIDADE, INTEGRIDADE E ANONIMIDADE NO SISTEMA DE VOTAÇÃO ELETRÔNICA DO BRASIL

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Engenharia de Software, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Me. Rodrigo Tomaz Pagno

Coorientador: Prof. Me. Newton Carlos Will

DOIS VIZINHOS

2019

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CÂMPUS Dois Vizinhos
Coordenadoria do Curso de Engenharia de Software

TERMO DE APROVAÇÃO

Autenticidade, Integridade e Anonimidade no Sistema de Votação Eletrônica do Brasil

por

Jessica Iara Pegorini

Este Trabalho de Conclusão de Curso foi apresentado em 27 de Novembro de 2019 como requisito parcial para a obtenção do título de Bacharel em Engenharia de Software. O(a) candidato(a) foi arguido(a) pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Rodrigo Tomaz Pagno
Presidente da Banca

Alinne Cristinne Correa Souza
Membro Titular

Andre Roberto Ortoncelli
Membro Titular

* A Folha de Aprovação assinada encontra-se na Coordenação do Curso

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me dado forças e coragem diante as dificuldades do dia a dia;

Agradeço a Universidade e o seu corpo docente que demonstrou estar comprometido com a qualidade e excelência do ensino;

Agradeço meu orientador pelo tempo, paciência e todo o ensinamento durante as diversas trocas de ideias;

Agradeço principalmente a minha família, meu pai Lauri e minha mãe Noeli, minha irmã Carla pela dedicação, cuidado, preocupação e principalmente por todo o amor, apoio e incentivo que me dedicaram durante todos esses anos;

Agradeço a todos os meus amigos que sempre estiveram comigo, aguentando crises de ansiedade, de estresse, de nervosismo e ao mesmo tempo compartilhando milhares de momentos de alegria, de conquistas, de histórias. Amigos de uma década de amizade ou amigos que chegaram recentemente. Amigos de longas conversas, de longas reflexões e de diversos momentos de descontração. Todos são muito especiais;

Agradeço a todos os colegas da UTFPR pelos momentos de aprendizado e principalmente as conquistas que compartilhamos;

Agradeço por todas as pessoas que passaram pela minha vida, e que de alguma forma e do seu jeito, me ensinaram alguma coisa;

A todos, meu muito obrigada.

"As máquinas me surpreendem muito frequentemente."

(Turing, Alan Mathison)

RESUMO

PEGORINI, Jéssica Iara. AUTENTICIDADE, INTEGRIDADE E ANONIMIDADE NO SISTEMA DE VOTAÇÃO ELETRÔNICA DO BRASIL. 118 f. Trabalho de Conclusão de Curso – Coordenadoria do Curso de Engenharia de Software, Universidade Tecnológica Federal do Paraná. Dois Vizinhos, 2019.

A tecnologia vem crescendo de forma gradativa nos últimos anos e cada vez mais os processos se tornam eletrônicos. Dessa forma, é de extrema importância que se estabeleçam alguns padrões de segurança aplicados a esses processos. A democracia é um dos processos que vem se tornando eletrônico com o passar dos anos, e o Brasil, como um dos países com a maior democracia do mundo, também aderiu ao processo de informatização do voto. É notório as vantagens que um processo de votação totalmente eletrônico traz para uma eleição. No entanto é importante ressaltar que além de vantagens, como a rápida apuração dos votos e disponibilidade dos resultados, existem problemas tecnológicos a serem tratados para evitar fraudes e falhas no sistema, garantindo um processo íntegro. Nesse sentido, o presente trabalho apresenta um mapeamento sistemático realizado na área da segurança eleitoral, que busca pelas principais informações sobre sistemas de votação eletrônica utilizados no mundo e um estudo de caso realizado com o objetivo de analisar quais são os problemas enfrentados no processo eletrônico brasileiro, para posterior comparação de ambos os sistemas. Os resultados apontam algumas semelhanças e diferenças entre os sistemas utilizados pelo Brasil e pelo mundo, como é o caso do sistema utilizado em alguns estados dos Estados Unidos da América. O sistema em questão apresenta uma grande variedade de mecanismos de segurança e é capaz de detectar fraudes, assim como o sistema eletrônico brasileiro, que também possui vários mecanismos de segurança, sendo capaz de detectar modificações não autorizadas. Por outro lado, o sistema utilizado pela Índia apresenta diferenças significativas quanto ao processo de autenticação do eleitor, uma vez que o Brasil adotou a biometria para esse processo, e a Índia utiliza uma tinta indelével para marcar os eleitores que são liberados para votar. O mais notável é a evolução tecnológica do Brasil, dado o destaque obtido na sociedade com a inserção da tecnologia no sistema eleitoral.

Palavras-chave: Voto eletrônico, Sistema Eleitoral, Segurança da Informação.

ABSTRACT

PEGORINI, Jéssica Iara. AUTHENTICITY, INTEGRITY, AND ANONYMITY IN BRAZILIAN ELECTRONIC VOTING SYSTEM. 118 f. Trabalho de Conclusão de Curso – Coordenadoria do Curso de Engenharia de Software, Universidade Tecnológica Federal do Paraná. Dois Vizinhos, 2019.

Technology has been growing gradually in recent years and more and more processes become electronic. Thus, it is extremely important that some safety standards be applied to these processes. Democracy is one of the processes that has become electronic over the years, and Brazil, as one of the countries with the largest democracy in the world, has also started the informatization of the vote process. The advantages that an all-electronic voting process brings to an election are notorious. However it is important to note that, in addition to advantages, such as rapid vote counting and the availability of results, there are technological issues to be addressed to prevent fraud and system failures, ensuring a fair process. In this sense, this paper presents a systematic mapping carried out in the area of electoral security, which seeks the main information about electronic voting systems used in the world, and a case study that analyzes what are the problems faced in the Brazilian electronic process, for later comparison of both systems. The results show some similarities and differences between the systems used by Brazil and the world, how is the case such as the system used in some states of the United States of America. The system in question has a wide variety of security mechanisms and is capable of detecting fraud, just as the Brazilian electronic system, which also has several security mechanisms, is capable of detecting unauthorized modifications. On the other hand, the system used by India presents significant differences in the voter authentication process, since Brazil has adopted biometrics for this process, and India uses an indelible ink to mark voters who are released to vote. Most notable is the technological evolution of Brazil, given the prominence obtained in society with the insertion of technology in the electoral system.

Keywords: Electronic Voting , Electoral System, Information Security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ACM	*Association for Computing Machinery*
BU	Boletim de Urna
CE	Critério de Exclusão
CI	Critério de Inclusão
CONFEA	Conselho Federal de Engenharia e Agronomia
CREA	Conselho Regional de Engenharia e Agronomia
IDEA	*Institute for Democracy and Electoral Assistance*
IEEE	*Institute of Electrical and Electronic Engineers*
IEC	*International Electrotechnical Commission*
ISO	*International Organization of Standardization*
MITM	*Man-in-the-Middle*
MPF	Ministério Público Federal
MS	Mapeamento Sistemático
OAB	Ordem dos Advogados do Brasil
QP	Questão de Pesquisa
RDV	Registro Digital do Voto
SA	Sistema de Apuração
SBC	Sociedade Brasileira de Computação
SBSeg	Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais
SYH	*Something You Have* (Algo que você tem)
SYA	*Something You Are* (Algo que você é)
TI	Tecnologia da Informação
TPS	Teste Público de Segurança
TRE	Tribunal Regional Eleitoral
TSE	Tribunal Superior Eleitoral
WTE	Workshop de Tecnologia Eleitoral

SUMÁRIO

1 INTRODUÇÃO

Com o crescente avanço da tecnologia, onde cada vez mais processos e sistemas vem sendo informatizados para atender as necessidades dos usuários. A segurança da informação se tornou um assunto de extrema importância no meio tecnológico, visto que ela é a responsável por assegurar a proteção dos dados do usuário, e garantir que estejam seguros de roubo, perda ou sequestro, e principalmente da divulgação dos mesmos sem o consentimento da vítima. Dessa forma, ela se tornou motivo de preocupação nos mais diversos segmentos de tecnologia.

Confidencialidade, integridade e disponibilidade, autenticidade e anonimidade são algumas das principais características que estão ligadas ao conceito de segurança da informação, e a quebra de um sistema de segurança pode levar uma organização a falência, por conta do impacto causado pela perda ou violação de dados (FAGUNDES, 2018).

A Associação Brasileira de Normas Técnicas (ABNT), por meio da Norma ISO/IEC 17799 de 2005, padroniza a informação como um ativo essencial para os negócios das organizações que pode se apresentar de diferentes formas, seja física, digital e até mesmo falada. De qualquer maneira que ela se apresente, ela deve ser protegida de forma adequada para evitar que ela seja perdida.

Um bom sistema de segurança é implementado por políticas, procedimentos e estruturas organizacionais e também contempla funções de software e hardware que precisam ser estabelecidas, implementadas e monitoradas para garantir que obtenham melhoramento caso necessário, para que a segurança das organizações seja atendida (NBR ISSO/IEC 17799:2005, 2005).

Tendo em vista que a segurança da informação está ligada a todo e qualquer sistema eletrônico, o sistema eleitoral adotado pelo Brasil é um exemplo de sistema que demanda fortes mecanismos de proteção contra a quebra de sigilo do processo. Um sistema que não implementa as propriedades de segurança, se torna um sistema passível de falhas, e é colocado em dúvida quanto a sua integridade. Para que uma eleição tenha credibilidade,

é necessário que ela se mostre transparente, íntegra e autentica e principalmente, que o eleitor tenha a certeza de que o seu voto é totalmente anônimo.

O Brasil é um dos países que utiliza sistema eletrônico na realização das eleições, mas antes de aderir à informatização do voto, esse já chegou a ser falado, e até que a urna eletrônica chegasse ao escopo que é conhecido hoje, ela passou por um longo processo de evolução. Atualmente elas são mantidas pelo Tribunal Superior Eleitoral (TSE), o qual é responsável por todo o processo eleitoral brasileiro, dessa forma, ele está sempre buscando o aprimoramento do sistema.

Segundo Aranha, Nunes e Cardoso (2018), o Brasil é uma das maiores democracias do mundo, onde cerca de 80% da população eleitoral participa ativamente das eleições que ocorrem de dois em dois anos. As urnas eletrônicas foram introduzidas no país em 1996, mas só no ano 2000 foi que as eleições se tornaram inteiramente eletrônicas no país. Embora o sistema de votação do Brasil seja, segundo o TSE, o mais "eficaz e independente sistema de votação do mundo", várias vezes as urnas eletrônicas utilizadas nas eleições brasileiras não passaram pelos testes de auditoria realizados por diversos profissionais da área de tecnologia da informação.

Tendo em vista que a votação tem o objetivo de garantir a anonimidade do voto do eleitor, é preciso entender de que que forma essa anonimidade pode ser garantida ao eleitor, e quais são as implicações de se utilizar um sistema eletrônico. Além disso, outras duas questões que precisam ser tratadas é: a confidencialidade do voto, que garante que os dados acerca deste voto somente serão conhecidos pelas entidades responsáveis; e a integridade do mesmo, que garante que o voto não sofreu modificações durante todo o processo eleitoral.

1.1 JUSTIFICATIVA

Múltiplas vulnerabilidades consideradas graves foram detectadas nos últimos Testes Públicos de Segurança da urna eletrônica brasileira, e quando combinadas elas podem comprometer desde o sigilo do voto, a integridade do software, até as principais propriedades de segurança do sistema (ARANHA; NUNES; CARDOSO, 2018).

Além disso, parte da sociedade ainda é cética em relação à confiabilidade do sistema de votação eletrônico, colocando em dúvida a lisura do processo. Sendo assim, alguns trabalhos já vem sendo desenvolvidos com o intuito de analisar a possibilidade de adulterações nos equipamentos utilizados durante o processo, como em Aranha, Nunes e

Cardoso (2018).

Dessa forma, também é de extrema importância efetuar uma análise de todo o processo eleitoral brasileiro, desde a efetivação do voto pelo cidadão, até a contabilização do resultado, de forma a identificar possíveis pontos de falha nesse processo. Outro ponto importante é fazer um levantamento sobre a democracia dos demais países do mundo, analisando quais são os meios utilizados para que a democracia seja colocada em prática, observando as dificuldades e as facilidades dos seus processos.

1.2 OBJETIVOS

O presente trabalho tem o intuito de contribuir com a segurança da informação, no sentido de explicar o atual processo eleitoral brasileiro, analisando a forma com que as eleições são realizadas e quais são os procedimentos adotados, e identificar por meio de um estudo de caso quais são os problemas enfrentados pela Justiça Eleitoral diante do sistema informatizado.

1.2.1 OBJETIVOS ESPECÍFICOS

Com base no objetivo geral são elencados os seguintes objetivos específicos que norteiam o presente trabalho:

- Analisar o ecossistema de votação eletrônica utilizado no processo eleitoral brasileiro;
- Apresentar as principais implicações quanto à integridade, confidencialidade e anonimidade sobre os dados resultantes do processo de votação;
- Mapear os sistemais eleitorais utilizados pelos demais países do mundo, e quais são os problemas enfrentados por eles;
- Realizar um estudo de caso para elencar as principais vulnerabilidades detectadas no sistema de votação eletrônica brasileiro;
- Realizar um breve comparativo entre o sistema brasileiro e os demais sistemas de votação eletrônica utilizados no mundo.

1.3 ESTRUTURA DO DOCUMENTO

O presente Capítulo traz uma introdução à Segurança da Informação, uma breve contextualização da problemática a ser abordada nesse estudo, juntamente com os objetivos a serem alcançados.

Em seguida, o Capítulo 2, apresenta uma breve descrição das principais características relacionadas a segurança da informação que serão levadas em consideração no desenvolvimento deste trabalho, relacionando-as com o atual sistema de votação eletrônico brasileiro, além de um apontamento das implicações causadas pela quebra dessas características. No Capítulo 3 é explanada a historia do voto no Brasil, a evolução do processo de informatização do voto que contempla também o surgimento e evolução da urna eletrônica utilizada nas eleições.

O Capítulo 4, realiza um mapeamento sistemático da literatura, que busca por evidências acerca de sistemas de votação eletrônica a nível mundial apresentando todo o processo realizado para a construção e desenvolvimento do mesmo, seguido pelos resultados alcançados. No Capítulo 5, é apresentado um estudo de caso que reúne as falhas detectadas no sistema brasileiro juntamente com as soluções implementadas pelo TSE.

No Capítulo 6 é feito um comparativo entre o sistema brasileiro e os sistemas eletrônicos utilizados pelos países retornados pelo mapeamento sistemático e por fim, o Capítulo 7 traz a conclusão deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Tendo em vista que a segurança da informação está ligada diretamente à proteção de dados do usuário, um sistema de votação eletrônica deve implementar características essenciais que assegurem que o eleitor tenha o seu voto preservado. A autenticidade, integridade e anonimidade são algumas das características mais importantes relacionadas ao processo eleitoral. Aliado à autenticidade, tem-se também o processo de autenticação do usuário, que garante que um eleitor não se passe por outro, impedindo o direito de outro eleitor. Essas questões são apresentadas nas seções seguintes.

2.1 AUTENTICIDADE

Uma das áreas mais conhecidas dentro da área da segurança da informação é a autenticidade, que é quem se responsabiliza por registrar um usuário que está enviando uma informação. Ela se refere a segurança da origem de toda e quaisquer informação, e possui a tarefa de garantir que uma pessoa é quem ela diz ser.

Para Marciano (2006, p.63) "a autenticidade é a garantia de que a informação é de fato originária da procedência alegada". Dessa forma, o meio mais comum de comprovar a autenticidade de informações, é por meio de assinaturas digitais.

Uma assinatura digital é resultado de mecanismos criptográficos, sendo utilizadas para verificação da autoria e autenticidade de documentos, que consiste no resumo digital do mesmo, cifrado com uma chave criptográfica privada do autor do documento (MAZIERO, 2017).

Dessa forma, a credibilidade e a segurança do processo eleitoral são demonstradas a partir autenticidade dos softwares utilizados pela urna eletrônica, confirmando que eles são de fato originais e oficiais, originados pelo TSE (Tribunal Superior Eleitoral, 2016a).

2.2 AUTENTICAÇÃO

Segundo Maziero (2017), a autenticação é uma técnica utilizada no processo de identificação e comprovação de entidades em um processo computacional. É dessa forma que um usuário que deseja se conectar a um sistema, comprova que ele é quem ele afirma ser. Para que os requisitos de segurança sejam atendidos é normal que um sistema computacional implemente mais de uma técnica de autenticação. Em um processo de votação, a identificação do eleitor é uma etapa crucial, que visa identificar o eleitor de forma inequívoca. Existem maneiras consideradas seguras utilizadas pela Justiça Eleitoral no processo de identificação e autenticação do eleitor no sistema eleitoral brasileiro.

A primeira técnica utilizada é a SYH - *Something You Have* (algo que você tem), composta por informações um tanto quanto complexas, baseadas em certificados digitais, cartões magnéticos, cartões de identificação entre outros. Embora robusta, essa técnica ainda possui pontos fracos, pois um cartão de identificação pode ser perdido, ou roubado e facilmente copiado por outro usuário mal intencionado. O sistema eleitoral brasileiro implementou por muito tempo esse tipo de autenticação, onde os eleitores eram identificados manualmente a partir do seu registro eleitoral e o porte de um documento oficial com foto. Esse processo era muito propenso a falhas, visto que eleitores mal intencionados poderiam autenticar-se apresentando uma documentação falsa aos mesários das seções eleitorais (MAZIERO, 2017).

A segunda forma de autenticação, se trata de SYA - *Something You Are* ("algo que você é"), a qual se baseia em características físicas associadas ao usuário, como seus dados biométricos que incluem a impressão digital, padrão da íris dos olhos, timbre de voz e etc. Apesar de ser uma técnica difícil de se implementar, ela é muito mais robusta quando comparada as outras, garantindo maior confiabilidade na autenticação de um usuário (MAZIERO, 2017).

No contexto eleitoral, a autenticação do usuário serve para identificar unicamente um eleitor perante a Justiça Eleitoral, e evitar que ocorra dele se passar por uma pessoa que não é. Por esse motivo, no ano de 2008 deu-se início uma etapa importante para a modernização do processo eleitoral. Se tratava de um projeto de Identificação Biométrica lançado pela Justiça Eleitoral, a qual utilizou-se da tecnologia para o reconhecimento individual do eleitor. Esse projeto tinha como principal objetivo garantir que cada eleitor seja único no cadastro eleitoral, e que no exercício do voto seja o mesmo que se habilitou no alistamento eleitoral. Nas eleições do ano 2016 cerca de 30% da população brasileira já

estava apta a votar por meio de identificação biométrica. Para o ano de 2018, os dados chegaram a marca de 50% da população. A autenticação biométrica tem como objetivo complementar a conferência manual de um documento de identificação, não eliminando a apresentação desse (Tribunal Superior Eleitora, 2018).

Considerando que a biometria vem sendo implantada com o intuito de diminuir o processo manual de identificação de eleitores, por meio de conferência de documentos, o risco de falhas em um sistema eleitoral sem um sistema de autenticação avançado, é muito grande. Se ocorre a quebra da autenticidade, pode ocorrer de um eleitor se passar por outra pessoa travós de documentação falsa, o que faz com que o verdadeiro eleitor perca o seu direito de exercer a cidadania.

2.3 INTEGRIDADE

A integridade da informação é a garantia de dados inalterados, o que significa que a mesma não foi modificada ou destruída sem a autorização. Ela é garantida quando não é roubada, corrompida, falsificada ou destruída no caminho entre origem e destino. Segundo Lyra (2015, p.40) "a integridade é responsável pela garantia que os dados são registrados por um processo ou indivíduo devidamente autorizado e reconhecido".

Existe alguns fatores que contribuem para a perda da integridade da informação, entre eles se encontram a substituição de parte do conteúdo da informação, alterações do seu elemento de suporte, o qual pode ocorrer na estrutura física e lógica onde ela está sendo armazenada, ou na má configuração de um sistema, podendo deixar informações restritas expostas (DANTAS, 2011).

Nesse sentido, a integridade tanto quanto a autenticidade garante ao eleitor que uma eleição não foi fraudada, e que o seu voto foi contabilizado corretamente. Um Sistema Eleitoral existe para que se promova o poder à uma pessoa de maneira pacífica e democrática, e isso só acontece quando uma eleição é realizada de forma íntegra, ou seja, de acordo com as regras que asseguram a pureza e a verdade do ato. Um sistema eleitoral perde a integridade quando é manipulado (ALVIM, 2015).

2.4 ANONIMIDADE

Outra propriedade da segurança da informação é a anonimidade, e está ligada diretamente ao usuário. Primeiramente é importante saber a diferença entre anonimidade e privacidade.

Anonimidade, permite que as ações de um usuário sejam vistas por outros usuários, sem que ele seja visto ou identificado. Já a privacidade deixa que o usuário seja identificado, porém as suas ações continuam protegidas dos demais usuários. Dessa forma, SYDON (2009) descreve a anonimidade como "a incerteza a respeito da identidade de um usuário".

Um sistema de votação eletrônica visa proteger o voto do eleitor, de modo a deixá-lo secreto, evitando que um eleitor sofra subornos ou ameaças na hora de escolher os seus candidatos. A anonimidade garante ao eleitor votar de acordo com a sua própria ideologia sem medo da influência de outras pessoas.

2.5 VOTO ELETRÔNICO

Segundo a Smartmatic (2018), o voto eletrônico é o termo utilizado para definir um processo de escolha, ou seja, uma eleição, que por sua vez pode utilizar meios eletrônicos para emitir, contar, e totalizar a quantidade dos votos. A votação eletrônica gera maior rapidez e agilidade na apuração dos votos, além de trazer maior acessibilidade para as pessoas que possuem algum tipo de deficiência, pois permite que elas possam exercer seus direitos de maneira independente. Na teoria, essas são características que asseguram a confiabilidade de um sistema de votação eletrônica (SMARTMATIC, 2018).

2.6 CONSIDERAÇÕES FINAIS

O presente capítulo apresentou de forma objetiva, as principais características da segurança da informação voltados ao ambiente eleitoral que serão abordados nesse trabalho. Visto que uma eleição tem o objetivo de eleger representantes partidários de forma democrática, o sistema de votação eletrônica tem o objetivo de garantir uma eleição íntegra, segura e transparente, assegurando a anonimidade do voto ao eleitor, que deve estar devidamente autenticado na hora de exercer a sua cidadania. Outro fator importante, se trata do software utilizado nas urnas eletrônicas, o qual também deve ser autêntico proveniente do TSE, autenticidade essa que se prova por meio de certificação digital.

3 VOTAÇÃO ELETRÔNICA NO BRASIL

Quando é preciso escolher um representante para ocupar algum cargo dentro de um grupo, existem diversos processos formais que podem ser adotados para auxiliar o processo, desde processos simples onde os grupos são pequenos e a democracia pode ser falada e expressada verbalmente, ou processos pouco mais complexos que podem envolver votação manual em papel, que posteriormente é conferido e divulgado por parte do grupo e podendo ser também registrado em ata. Quando se trata de escolha de representantes para grupos maiores, esse processo manual acaba ficando dificultado, dependendo do tamanho do grupo ou do tipo de escolha que se está realizando. Um exemplo para tal complexidade, é o processo de escolha de alguém que vai representar uma cidade, pois dependendo do numero de habitantes, uma votação em papel acaba se tornando um processo custoso e duvidoso, visto que a conferência manual dos votos acaba se tornando algo que põe em dúvidas os resultados.

Esse processo fica ainda mais complexo quando se trata de uma eleição ainda maior, como é o caso da escolha de alguém que vai representar o país. Dessa forma, há anos atrás inventores e pesquisadores começaram a pensar em formas automatizar esse processo, tornando-o mais confiável e transparente. Foi assim que, anos depois surgiu a ideia da informatização do voto. Em seguida as urnas eletrônicas começaram a ser moldadas com intuito de eliminar a intervenção humana no processo eleitoral. Desde a criação do primeiro protótipo, até que se chegasse as urnas eletrônicas que conhecemos hoje, elas passaram por um longo processo de evolução. Dessa forma, o ano de 2019 marca 23 anos da existência das urnas eletrônicas brasileiras.

Este Capítulo aborda a história da votação eletrônica no Brasil e as características da urna eletrônica e do processo eleitoral brasileiro, a fim de esclarecer de que forma acontece uma eleição. Sendo assim, a Seção 3.1 apresenta um breve histórico sobre a informatização do voto, seguido pela surgimento da urna eletrônica utilizada no sistema eleitoral brasileiro e sua evolução na Seção 3.2. A Seção 3.3, contempla a infraestrutura do processo. Seguido pela acessibilidade na Subseção 3.3, e Zerésima e Boletim de Urna na

Subseção 3.3.2. Os processos que envolvem a totalização dos resultados e o armazenamento e suprimento das urnas eletrônicas são apresentados nas Subseções 3.3.3 e 3.3.4, e por fim a Seção 3.4 apresenta as considerações finais do referido Capítulo.

3.1 HISTÓRIA

Houve um tempo em que o voto do eleitor era falado para um escrivão que anotava e depois o apurava, anotando os nomes dos eleitores em papel guardados em bolas de cera, conhecidos como pelouros. Essas bolas de cera, ficavam guardadas em arcas de madeira até o dia em que a comunidade pudesse saber os resultados. No tempo do Império e nos primeiros anos de república, não havia cédula oficial de votação, nesse caso, os eleitores depositavam em urnas de madeira qualquer papel com o nome do candidato. A escolha também poderia ser feita apenas se o eleitor falasse em voz alta o nome do seu candidato, pois era válido pela legislação da época (FUCK et al., 2016).

O sigilo do voto passou a ser garantido no ano de 1932 com a criação da Justiça Eleitoral, que trouxe as cabines indevassáveis e as sobrecartas oficiais para votação. As cédulas de votação, mesmo que sendo fabricadas pelos candidatos, agora eram depositadas nas urnas pelo eleitor dentro de envelopes opacos fabricados pela Justiça Eleitoral. Em 1955 a cédula de votação oficial começou a ser utilizada com a finalidade de coibir fraudes e minimizar a influência do poder econômico nos pleitos eleitorais, pois isentava os candidatos de fabricarem as cédulas de votação (FUCK et al., 2016).

O Código Eleitoral de 1932 responsável pelo voto secreto, trouxe a previsão da utilização de máquinas de votar, através do artigo 57 onde diz: "Resguarda o sigilo do voto, o uso das máquinas de votar, reguado oportunamente pelo Tribunal Superior, de acordo com o regime deste Código". Dessa forma, a luta pela automatização do sistema eleitoral nos anos seguintes, levou a construção de muitos projetos de máquinas de votar, as quais foram apresentados ao TSE. Porém, antes das urnas eletrônicas que conhecemos atualmente, nenhum outro projeto foi de fato concretizado (CABRAL, 2004, p.124).

O inventor mineiro Sócrates Ricardo Puntel, foi um dos primeiros a projetar um modelo de máquina de votar no ano de 1958, apresentando-o a vários órgãos da Justiça Eleitoral, e insistindo nas vantagens ligadas a agilidade e segurança do seu invento. A máquina de Puntel, como ficou conhecida, funcionava a partir de duas teclas e duas réguas que indicavam os cargos a serem preenchidos. Apesar de engenhoso, o equipamento pesava cerca de 35 quilos, o que tornava-o inacessível. Após seus protótipos serem reprovados

diversas vezes por ineficiência, ele acabou desistindo e abandonando o projeto (SILVEIRA, 2011).

Em 1974, foi a vez do advogado gaúcho Francisco Moro sugerir um novo sistema eletrônico, o qual se tratava de um modelo semelhante ao utilizado nas loterias esportivas, que também era novidade na época. Seu projeto consistia em um cartão que seria assinalado pelo eleitor, perfurado pelo mesário no final da votação, e enviado a um computador capaz de fazer a decodificação dos bilhetes. Segundo Moro, o modelo seria de fácil uso por parte dos usuários, e as vantagens desse novo sistema consistia em repercussão internacional, economia de pessoal, segurança, rapidez e exatidão na apuração dos resultados, principalmente agilidade na contagem e divulgação dos resultados.

Ele apresentou o seu protótipo ao Juiz Eleitoral do município de Osório no Rio Grande do Sul. e depois o projeto foi encaminhado ao TSE para ser analisado. Por coincidência, nesse mesmo ano o TRE do Rio Grande do Sul realizou a contagem final dos votos utilizando computadores, fruto de um convênio entre o TRE e o Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul.

Treze anos mais tarde, em 1987, o Engenheiro Civil Alberto Gosch sem ter conhecimento do projeto apresentado por Moro, pensou em um sistema semelhante, levantando a possibilidade do voto seguir por caminhos parecidos com os utilizados nos cartões da loteria, e reforçou o uso da tecnologia no processo eleitoral. Gosch estudou o tema durante um ano, e em dezembro de 1988 apresentou seu projeto ao TRE do Rio Grande do Sul via ofício. Três dias mais tarde foi notificado pelo mesmo, que essa possibilidade já estava em estudo no TSE (SILVEIRA, 2011).

Depois da máquina de Puntel, vários outros Tribunais Regionais Eleitorais (TRE) tentaram desenvolver ideias para a automatização do processo eleitoral. Em 1983 o TRE do Rio Grande Do Sul começou a realizar o cadastramento dos seus eleitores. Foi só em 1986 durante a presidência do Ministro Néri Silveira, que a Justiça Eleitoral Brasileira aderiu ao processo de informatização do voto, e começou a realizar o recadastramento eletrônico dos eleitores, abrangendo cerca de 70 milhões de pessoas. Esse procedimento foi implantado a fim de impedir que um eleitor se cadastrasse em mais de um estado, evitando o voto repetido (TAVARES, 2011, p.15).

A cidade de Brusque em Santa Catarina, organizou uma seção informatizada no ano de 1989, onde os eleitores utilizaram um computador que estava em caráter experimental para o segundo turno das eleições presidenciais daquele ano, enquanto isso um microcomputador modelo 386 instalado no TSE recebeu o repasse das informações.

Esse foi o ponta pé inicial para o aceleramento do processo de informatização do voto no estado, onde nos dois anos seguintes já conseguiu instalar um microcomputador em cada uma das zonas eleitorais (SILVEIRA, 2011, p.22).

Segundo dados do TRE de Santa Catarina, a "primeira votação totalmente eletrônica da América Latina", foi realizada no interior do estado no dia 31 de março de 1991, e tratava-se de uma consulta acerca da emancipação do Distrito de Cocal do Sul. Mas a primeira eleição de presidenciáveis ocorreu de fato somente no ano de 1995 nas eleições municipais da cidade de Xaxim, oeste catarinense, onde já era possível visualizar a fotografia dos candidatos na tela do computador (Tribunal Regional de Santa Catarina, 2015).

Em 1994, aconteceu pela primeira vez a totalização das eleições gerais utilizando um computador central no TSE, durante a gestão do Ministro Supúlveda Pertence. Somente no ano seguinte, quando O Ministro Carlos Velloso estava à frente da Gestão do TSE foi que o processo de informatização do voto iniciou de fato, quando uma comissão de juristas e técnicos de TI apresentaram um protótipo de urna eletrônica. Para a elaboração do projeto da urna, incluindo os programas necessários para o seu funcionamento, montou-se um grupo de trabalho que contava com técnicos e especialistas em informática, comunicação e eletrônica da Justiça Eleitoral, Forças Armadas, Ministério da Ciência e Tecnologia e Ministério das Comunicações.

Paralelamente a isso o TSE procurava sensibilizar além da Justiça Eleitoral, os demais poderes, Legislativo e Executivo, quanto ao grandioso empreendimento, visto que dependia tanto da adequação da lei de implantação do voto eletrônico, quanto do fornecimento de recursos financeiros necessários. Em cinco meses o projeto foi concluído, e a urna eletrônica criada pelo TSE foi licitada para fabricação.

O objetivo inicial era adquirir urnas capazes de registrar o voto de pelo menos um terço do eleitorado, o que equivalia a cerca de 100 milhões de pessoas. Durante as eleições desse ano, o voto eletrônico abrangeu todo o estado do Rio de Janeiro e todas as capitais brasileiras. Os municípios com mais de 200 mil eleitores também adotaram o sistema eletrônico naquele ano (Tribunal Superior Eleitora, 2018).

A única exceção à regra dos municípios com mais de 200 mil eleitores adotarem a eleição por meio do sistema eletrônico, foi o município de Brusque, que foi a primeira cidade do país a utilizar a informática nas eleições. A partir desse ano, a informatização das eleições avançou de forma progressiva, atingindo o seu ápice nas eleições do ano 2000, onde o processo eletrônico foi estendido a todas as zonas eleitorais do país. Já nos anos

seguintes, 2002, 2004 e 2006 todo o eleitorado votou por meio eletrônico (Tribunal Regional de Santa Catarina, 2015).

Segundo o TSE, o voto eletrônico é visto como uma solução universal para a democracia do país, onde implementa características de autonomia, facilidade na logística, custo reduzido, segurança entre outros, e destaca que todo o processo de informatização tem sido altamente estudado, visando a segurança e transparência do processo. No ano de 2008, a Justiça Eleitoral iniciou uma etapa de modernização do processo eleitoral quando lançou o projeto da Identificação Biométrica, utilizando-se da tecnologia para o reconhecimento individual do eleitor. O projeto vem sendo realizado com sucesso desde então, onde o cadastramento biométrico e a leitura das digitais envolveram inicialmente cerca de 40 mil eleitores de Santa Catarina, Mato Grosso do Sul e Rondônia. Em 2014 já eram mais de 21 milhões de eleitores com identificação biométrica cadastrada (Tribunal Superior Eleitora, 2018).

3.2 URNA ELETRÔNICA

Segundo o TSE esse modelo de urna eletrônica é um dos mais modernos sistemas já implantados no mundo, pois seus confiáveis mecanismos eletrônicos de coleta e conferência de votos conseguem anunciar os resultados em poucas horas após o encerramento das votações, e já é utilizado por diversos países do mundo, como Suíça, Canadá, Austrália e alguns estados dos Estados Unidos, entre outros (Tribunal Superior Eleitora, 2018).

A urna que conhecemos hoje começou a ganhar forma no ano de 1995, a partir de um projeto criado pelo TSE, e apesar de possuir várias versões, todas as urnas eletrônicas são compostas por um terminal eleitoral usado para identificar o eleitor, e outro para identificar o lançamento dos votos. Esses dois equipamentos são conectados por um cabo, e assim que o eleitor é identificado os seus dados aparecem na tela do segundo terminal, onde os votos são recebidos via teclado (ARANHA; RIBEIRO; PARAENSE, 2016).

Desde que foi concebida, a urna eletrônica já passou por várias versões. Em 1996, a urna utilizada pela primeira vez em eleições municipais, se tratava do modelo **UE 1996**, e abrangeu cerca de 32% do eleitorado. Essa versão possuía uma pequena impressora destinada ao registro do voto os quais eram destinados a uma pequena caixa de plástico acoplada a urna. Na tela aparecia somente as fotos dos candidatos aos cargos majoritários.

Em seguida, o modelo **UE 1998** a capacidade do processamento e a memoria foram ampliados em relação ao modelo UE 1996, permitindo o registro fotográfico de todos

os candidatos. Nessa época já havia sido extinto o voto impresso, e cerca de 57,6% do eleitorado nacional votou utilizando esse modelo de urna.

O modelo seguinte, **UE 2000** contava com uma novidade, a criação da saída de áudio para fones de ouvido. Funcionalidade essa que foi desenvolvida e aprimorada visando os eleitores que possuem deficiência visual. Nesse ano, o voto utilizando urnas eletrônicas abrangeu 100% do eleitorado.

O voto impresso foi instituído novamente no ano de através da Lei nº.10.408/2002, porém a diferença do do modelo **UE 2002** para o modelo de 1996, foi a previsão de que o eleitor poderia conferir visualmente o voto impresso. Outra alteração, foi a adoção do sistema operacional Windows CE que veio substituindo o VirtuOS.

O modelo **UE 2004** substituiu o mecanismo de impressão de voto, pelo Registro Digital do Voto - RDV, um arquivo digital que é responsável por armazenar todos os votos. Outra inovação desse período foi a previsão de que a Ordem dos Advogados do Brasil - OAB, Ministério Público e partidos políticos poderiam participar das fases de especificação e desenvolvimentos dos programas de computador utilizados na Urna eletrônica.

Posteriormente, o modelo **UE 2006** contou com uma importante inovação, o leitor biométrico de impressão digital para a autenticação do eleitor no terminal do mesário. Porém essa novidade só começou a ser usada a partir do ano de 2008, quando a Justiça Eleitoral deu inicio ao processo de recadastramento biométrico, pois até então a identificação e autenticação do eleitor era feita pelos mesários da seção eleitoral, através do registro eleitoral do eleitor e a conferência de um documento oficial com foto. Atualmente, em alguns estados do Brasil, esse processo vem sendo realizado via biometria, resultado desse projeto criado pela Justiça Eleitoral.

Depois foi a vez do modelo **UE 2009**, onde houveram importantes inovações técnicas: Inserção do leitor de *smart card* e o *display* gráfico de apresentação da foto do eleitor no terminal do mesário, *pen drives* de 128 MB de espaço passaram a armazenar as memórias de resultado e o sistema windows foi substituído pelo Linux para que o TSE tivesse uma adaptação e modificação completa do programa.

Por fim, os últimos modelos fabricados foram o **UE 2011** e **UE 2013** os quais possuem um leitor biométrico de maior qualidade, além de um botão de liga e desliga que substituiu o antigo método de acionamento das urnas, que antes era realizado através de uma chave física (FUCK et al., 2016).

O ex-juiz eleitoral do Paraná, Sergio Bernardinetti, descreve as urnas eletrônicas

como computadores que rodam com um sistema operacional baseado em Linux, o qual foi desenvolvido inteiramente por técnicos da Justiça Eleitoral. Além dele rodar em uma placa de sistema bem simples, ele possui ainda um cartão de memória principal e executa somente o programa de votação. Elas não contam com nenhum tipo de hardware de rede, tornando impossível conecta-la com internet, *bluetooth* ou outros dispositivos, e a partir das 17 horas imprimem o Boletim de Urna (BU), o qual revela o total de votos recebidos de forma detalhada, e não aceita mais nenhum voto. Durante o processo de votação, os votos vão sendo armazenados em *pen-drives* especiais, identificados pela cor laranja. Eles são criptografados e lacrados, cujo lacre também leva a assinatura do Juiz e do Promotor Eleitoral (BERNARDINETTI, 2018).

Segundo Fuck et al. (2016), as urnas eletrônicas foram criadas seguindo 8 diretrizes que garantiram o sucesso do produto e a tornaram simbolo das eleições brasileiras, essas diretrizes são:

- Solução universal: registra o voto pelo número do candidato, ou pelo número do partido;
- Aderência à legislação vigente: a máquina foi criada com a capacidade de evolução para garantir que mudanças na legislação eleitoral não exigissem alterações na urna;
- Processo amigável: O equipamento é de fácil utilização para facilitar o processo de votação para o eleitor, que pode visualizar a foto do seu candidato na tela da urna antes de confirmar o voto;
- Custo reduzido: O projeto tem um custo economicamente viável, mesmo com o elevado número de seções eleitorais;
- Perenidade: Possibilita o uso em várias eleições, o que diminui o custo do voto;
- Segurança: O equipamento elemina o risco de fraude no registro de voto e na apuração dos resultados;
- Facilidade na Logística: A urna é pequena e robusta, pesa pouco e é de fácil armazenamento e transporte; e
- Autonomia: Possui bateria para localidades que não possui energia elétrica, ou para casos isolados de queda de luz.

Para cada eleição as urnas são carregadas com um conjunto de 28 aplicativos desenvolvidos pelo TSE que formam o "ecossistema da urna". Esses aplicativos são responsáveis pela automatização das atividades e dos processos para o seu bom funcionamento, dentre eles destacam-se:

- Gedai-UE - Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica que se responsabiliza pelos *flashes* de carga, de votação e mídias para a urna, além de receber e enviar as correspondências para os TREs.
- SCUE - Sistema de Carga de Urna Eletrônica responsável por instalar o sistema operacional, os dados de eleições, gerando um número único relativo a cada urna.
- Atue - Sistema de Auto teste da Urna Eletrônica, o qual é responsável por realizar auto teste para verificação dos componentes da urna a fim de verificar se estão funcionando devidamente.
- Vota – Sistema responsável por coletar e apurar os votos de uma seção eleitoral.

Além do Ecossistema da Urna, elas ainda contam com um conjunto de 90 sistemas destinados às urnas eletrônicas, que são lacrados e enviados aos TREs para que prossigam com a instalação individual em cada uma das urnas. Além disso, cada urna também recebe as informações a respeito dos candidatos e cartões de memória que armazenam uma cópia dos votos no dia da eleição (Tribunal Superior Eleitora, 2018).

Todos os sistemas utilizados pela urna são lacrados e assinados digitalmente na Cerimônia de Assinatura Digital e Lacração dos Sistemas, evento público exigido por lei que acontece no TSE, e participam partidos políticos, coligações, Ministério público, Ordem dos Advogados do Brasil e pessoas autorizadas. Nessa ocasião são gerados o *hash* dos programas lacrados, para que se possa ser comprovada a autenticidade da urna eletrônica a qualquer momento.

A lista de *hashes* é distribuída e disponibilizada no portal do TSE, para que se possa conferir a qualquer momento e de qualquer parte do Brasil se o *hash* do programa utilizado na urna é o mesmo gerado na cerimônia pública. A alteração de apenas um caractere do código fonte dos sistemas, gera incompatibilidade com o *hash* original, o que comprova a adulteração da urna eletrônica (FUCK et al., 2016).

Além da segurança digital, as urnas eletrônicas contam ainda com práticas e dispositivos para assegurar que ela não seja fisicamente violada. O projeto da urna é de total controle do TSE, dessa forma a empresa responsável pela fabricação dos componentes

físicos e pela montagem das mesmas, não consegue utilizar a máquina sem uma autorização prévia da Justiça Eleitoral.

Ela está preparada para enfrentar todos os tipos de condições climáticas, de armazenamento e de transporte pelo Brasil. Quando pronta para votação, recebe um lacre de segurança fabricado pela Casa da Moeda brasileira, o que evidencia qualquer tentativa de violação. Além disso, a urna possui um *log*, onde são registrados os eventos pra posterior análise, que identifica os eventuais problemas que possam ter ocorrido durante a votação.

Antes dos eleitores começarem a votar no dia da eleição, a urna imprime a zerésima, que comprova que a mesma não possui nenhum voto, e ao final da votação, imprime os boletins de urna, relatório esse que contém a totalização de votos registrados na seção. Também é importante destacar, que as urnas não possuem qualquer tipo de rede de dados, para impedir qualquer ataque via internet (FUCK et al., 2016).

A atual urna utilizada nas eleições brasileiras é um microcomputador que possui mecanismos que a tornam a máquina ideal para a computação dos votos. Conforme mostra a Figura 1, ela é constituída por:

1. Memória de resultado: uma espécie de *pen drive* um pouco maior que um *pen drive* tradicional, de fácil encaixe a urna. É o mesário que o encaixa na urna no dia da eleição;

2. Impressora térmica: Uma pequena impressora semelhante as utilizadas em máquinas de cartão de crédito, que é responsável pela impressão do BU. Utiliza um papel especial que faz com que o dados impressos nele durem por até cinco anos;

3. Cabos de alimentação: Cabos de energia que mantém a urna ligada á energia elétrica;

4. Bateria interna: Bateria que possui duração de até 13 horas que se aciona quando há falta de energia no local de votação;

5. Bateria Externa: para o caso de falta de luz na seção e a bateria externa acabar, existe uma terceira com duração próxima a da interna;

6. Memória *flash*: Além da memória de resultado, a urna também grava os dados em um cartão de memoria *flash* que garante a redundância dos dados caso a outra memória sofra algum problema;

7. USB: É possível salvar os dados da urna em *pen drives* . Essa medida serve para garantir a redundância dos dados registrados; e

8. Saída de Áudio: Há uma saída de áudio compatível com a maioria dos fones de ouvido comuns, que serve para auxiliar eleitores com deficiência visual. Ao conectar um fone o eleitor escuta os números que digitou na urna.
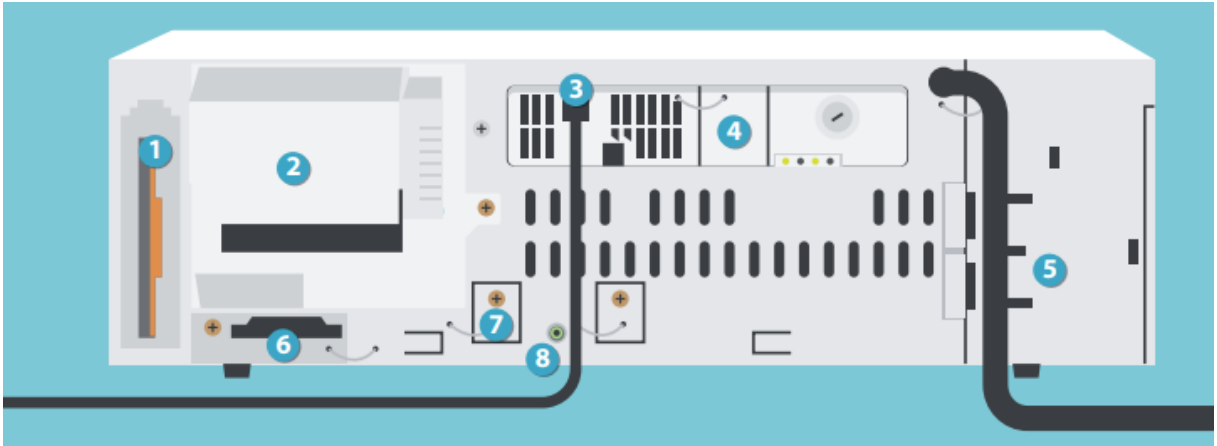
Figura 1: Componetes da atual urna eletrônica brasileira.
Fonte: Fuck et al. (2016)

O terminal do mesário é quem comanda a eleição, pois é a partir dele que o eleitor é liberado para votar. O mesário digita o número do título do eleitor para confirmar a sua identidade, e então o libera para votar. Quando a eleição termina o mesário digita a senha responsável por comandar que a impressão do BU inicie. O terminal do mesário é composto por:

1. Impressão digital: Leitor biométrico para confirmar a identidade do eleitor; e

2. Teclado: Composto por teclas enumeradas de 0 a 9, dois botões, um de confirma e outro de corrige, tela e luzes de led que indicam se a urna está liberada ou aguardando, e também o nível de bateria.

3.3 INFRAESTRUTURA

O processo eleitoral é organizado pela Justiça Eleitoral em nível municipal, estadual e federal, e cabe a ela organizar, fiscalizar e realizar o processo eleitoral bem como a situação dos partidos e dos candidatos. Seu órgão máximo o TSE, com cede em Brasília, e cada estado brasileiro possui um TRE que conta com juízes e juntas eleitorais. Todo o processo eleitoral é dividido por fases.

Figura 2: Terminal do Mesário.
Fonte: Fuck et al. (2016)

Depois de realizado a cerimonia pública de Assinatura Digital e Lacração dos sistemas, os softwares são liberados para que os TREs para a instalação e importação dos dados eleitorais, que novamente em cerimonias públicas preparam as urnas com os dados para a eleição. Existem dois tipos de mídia com que a urna trabalha: a *flash card* em formato de cartão de memória, e a memoria de resultado, em formato exclusivo da Justiça Eleitoral, que é uma espécie de *pen drive.*

A preparação das urnas em cada seção é realizada em duas etapas, que fazem a instalação do sistema operacional, programas e bibliotecas além dos dados eleitorais fazendo utilização dos cartões de memória de carga, e a segunda etapa que contempla a realização dos testes para comprovar o completo e correto funcionamento das urnas utilizando os cartões de votação e as memórias de resultado. Em seguida, as urnas são encaminhadas para armazenagem em locais designados pelo TRE de cada estado, e na véspera da eleição são transportadas para os locais de votação (FUCK et al., 2016).

3.3.1 ACESSIBILIDADE

A votação é a fase mais conhecida pelos cidadãos, pois é o momento em que os representantes políticos são escolhidos pela população. A Justiça Eleitoral Brasileira é referência pelo mundo pela promoção da votação segura realizada pela urna eletrônica, e pela garantia da acessibilidade de todos os eleitores com algum tipo de deficiência, através de mecanismos que garantem que o cidadão poderá acessar o local de votação tranquilamente. Alguns desses cuidados, envolvem o atendimento prioritário a gestantes, cadeirantes, maiores de 60 anos e pessoas com mobilidade reduzida.

Além do mais, o eleitor que possui qualquer tipo de deficiência, pode requerer a transferência do local de votação para uma seção especial, que melhor possa atender as suas necessidades. Esse processo pode ser feito no cartório eleitoral em até 151 dias antes do dia da eleição. Com 90 dias de antecedência, os eleitores com deficiência que votam em seções especiais, podem comunicar por escrito o juiz eleitoral acerca das suas necessidades, para que a zona eleitoral do eleitor seja adequada da melhor forma possível.

Se o eleitor não realizou o pedido escrito ao juiz eleitoral, ele poderá fazer o requerimento com os mesários da zona eleitoral no dia da votação, e pode ainda contar com a ajuda de uma pessoa de sua confiança, autorizada pelo presidente da mesa receptora, para que lhe preste ajuda se necessário. As urnas também são preparadas para atender eleitores com deficiência visual, que além do sistema de braile, contam com fones de ouvido nas seções eleitorais especiais, disponibilizados pelos Tribunais Eleitorais.

No caso dos eleitores analfabetos, o voto é facultativo, e mesmo que um eleitor nesta condição decida votar, a assinatura pode ser feita usando a digital do polegar direito. (Tribunal Superior Eleitora, 2018).

3.3.2 ZERÉSIMA E BOLETIM DE URNA

Uma das medidas que garantem a segurança e a confiabilidade do processo eleitoral é a impressão da zerésima, um relatório gerado depois da inicialização de cada urna eletrônica, o qual mostra que a urna está zerada. Esse documento é assinado pelo presidente da mesa receptora, pelo secretário e pelos fiscais dos partidos que estejam presentes na seção.

Ao final do dia e com a votação concluída, são impressas 5 vias obrigatórias do BU, os quais contém todas as informações da seção eleitoral. Além dos 5 obrigatórios, também podem ser impressos mais 15 cópias adicionais. Segundo informações do Tribunal

Superior Eleitoral (2019a), o BU é criptografado, assinado digitalmente e só então ele é transmitido ao sistema totalizador, responsável por validar a compatibilidade da chave pública de assinatura digital do BU com a sua chave privada e fazer a descriptografia do mesmo para a recuperação dos dados.

O RDV é o arquivo responsável por registrar todos os votos dos eleitores, e é a partir desse arquivo que a zerésima e o BU são emitidos. Ele registra exatamente e somente o que foi digitado na urna, e só é utilizado no fim da eleição para a emissão do BU. Ele não registra nenhuma informação adicional, o que torna impossível vincular o voto com um respectivo eleitor. Esse arquivo, é um instrumento muito importante para a realização de auditorias e verificação da apuração de uma seção. Esse arquivo garante o sigilo do voto do eleitor, pois cada voto é armazenado em uma posição aleatória do arquivo, o que torna impossível a vinculação desses votos com a sequência de comparecimento dos eleitores (Tribunal Superior Eleitora, 2018).

3.3.3 TOTALIZAÇÃO E TRANSMISSÃO DOS RESULTADOS

As eleições encerram-se às 17 horas nas seções eleitorais, horário que o presidente da mesa receptora de votos gera o BU, através de uma senha própria. Das cinco vias obrigatórias impressas, três são encaminhadas ao Cartório Eleitoral, uma fica fixada no local da votação, e a última é entregue para os representantes partidários.

Os dados armazenados nas urnas, são assinados digitalmente e gravados na mídia de resultados, a qual é criptografada na linguagens dos programas de computador utilizados pelo TSE. Esses dados são enviados aos polos de transmissão por meio de uma rede criptografada de uso exclusivo da Justiça eleitoral.

Os Tribunais contam com mecanismos de segurança desenvolvidos pela Justiça eleitoral responsáveis por assegurar que as informações que saem da urna cheguem ao seu destino sem qualquer alteração. O canal de transmissão por onde passam os dados também recebem uma camada de criptografia, inviabilizando ataques externos. Os TREs ainda realizam a verificação dos dados para conferir a integridade dos mesmos, através da decifração dos arquivos e verificação da assinatura digital, para comprovar que os dados recebidos são provenientes das urnas eletrônicas da justiça eleitoral.

A totalização dos resultados, começam no centro de processamento de dados do TRE de cada estado Brasileiro, onde os servidores da Justiça Eleitoral usam ferramentas computacionais para o processo de contagem e verificação dos votos das urnas de todo

estado, a fim de comprovar a confiabilidade, que assegura que o resultado é íntegro, oriundo de uma urna eletrônica preparada pela Justiça Eleitoral. Cada uma das etapas de transmissão possui um conjunto de chaves próprias e únicas que garantem a integridade dos dados.

Os arquivos são verificados via assinatura digital e os BUs são decifrados com chave de propriedade dos sistemas de totalização, o que tornam o BU legível. Quando os dados estão em consonância, já seguem para totalização e divulgação. Votos nulos e brancos não são considerados no somatório dos votos válidos. Os resultados da disputa presidencial, são encaminhados ao TSE em Brasília, o qual é responsável pela totalização e divulgação, que acontece em tempo real, sendo possível acompanhar minuto a minuto a evolução da apuração (Tribunal Superior Eleitora, 2018).

3.3.4 ARMAZENAMENTO E SUPRIMENTO DE URNAS ELETRÔNICAS

A Justiça Eleitoral possui cerca de 500 mil urnas eletrônicas armazenadas nos TREs e no TSE, as quais ficam guardadas em ambiente climatizados e em estruturas de madeira. De 4 em 4 meses são realizados testes e carregamento das baterias. No ano que antecede uma eleição, o TSE entra em contato com os TREs para verificar a necessidade de aquisições de mais urnas. E após isso, é responsabilidade de cada TRE encaminhar as urnas para as seções eleitorais.

A compra e controle das urnas fica a encargo do TSE, que realiza licitações para a aquisição, e realiza auditorias durante o processo de fabricação para garantir a padronização e a segurança das mesmas. É importante ressaltar, que apenas o hardware é contratado, pois todos os sistemas que compõe a urna eletrônica são desenvolvido exclusivamente pelo TSE.

Já a logística de distribuição para os locais de votação, dependem das necessidades de cada TRE e de cada zona eleitoral. Alguns tribunais fazem a entrega das urnas aos presidentes da mesa receptora, o qual fica encarregado de guardar a urna e montar a seção eleitoral no dia da eleição. Em locais distantes e de difícil acesso, a Justiça Eleitoral conta com o apoio da Marinha e da Aeronáutica, além de contratar empresas especializadas em transportes para garantir que s urnas e os kits de transmissão via satélite cheguem com segurança ao seu destino. Muitas delas podem ser transportadas por barcos, helicópteros ou aviões, e em alguns lugares com condições extremas de transporte, elas são levadas a pé (Tribunal Superior Eleitora, 2018).

A cada 10 anos, as urnas podem ser enviadas para reciclagem ou reutilização dos seus componentes. Todo o processo é feito com muito cuidado pela Justiça Eleitoral que se preocupa também com a preservação ambiental. O que não pode ser reciclado, são descartados em ateros sanitários credenciados, que seguem uma série de medidas de segurança. Para cuidar desses detalhes, o TSE realiza licitações, e as empresas que as ganham devem comprovar que os materiais foram devidamente encaminhados ao destino correto através de relatórios detalhados do que foi feito (FUCK et al., 2016).

3.4 CONSIDERAÇÕES FINAIS

Após o Código Penal de 1932 prever o uso de máquinas de votar para agilizar o processo eleitoral brasileiro, diversos inventores começaram a desenvolver e apresentar protótipos de máquinas de votar aos TREs, dos quais muitos foram rejeitados por ineficiência. Foi o ano de 1995 que ficou marcado pelo início do processo de informatização do voto que conhecemos, quando o TSE montou um grupo e trabalho que contava com técnicos e especialistas da Justiça Eleitoral, Formas Armadas, Ministério da Ciência e Tecnologia e o Ministério das Comunicações para o desenvolvimento do sistema de votação eletrônica que conhecemos hoje.

A urna eletrônica utilizada hoje foi desenvolvida pelo TSE e conta com dois terminais de identificação, um para identificação do eleitor e o outro para identificar o seu voto. Possui um Ecossistema de Urna composto por 28 aplicativos de automatização além de um conjunto de 90 sistemas específicos que garantem a automatização dos processos eleitorais. No âmbito de infraestrutura, o processo eleitoral é dividido por fazes, que vão desde o processo de votação em si, momento em que os eleitores se dirigem até as seções eleitorais para depositar o seu voto na urna, até o momento que em a totalização desses votos é realizada na sede do TSE em Brasília.

A Figura 3 ilustra o processo de apuração, totalização e divulgação dos resultados de uma eleição. No final da eleição os dados são assinados digitalmente e gravados em uma mídia de resultado, destacando-se que o BU além de assinado é também criptografado. Então o VOTA (sistema responsável pela coleta e apuração dos votos) grava as informações na mídia de resultados que são encaminhadas ao local próprio para transmissão. No caso das localidades de difícil acesso, como aldeias indígenas e certas comunidades ribeirinhas, essa transmissão é feita via satélite para o respectivo TRE ou zona de votação.

Depois de receber os dados, os TREs dão início ao procedimento de totalização

dos votos através da soma de todos os boletins de urna e, em seguida os resultados são divulgados. É importante ressaltar que tanto o voto nulo como o voto em branco não são considerados na soma dos votos válidos.
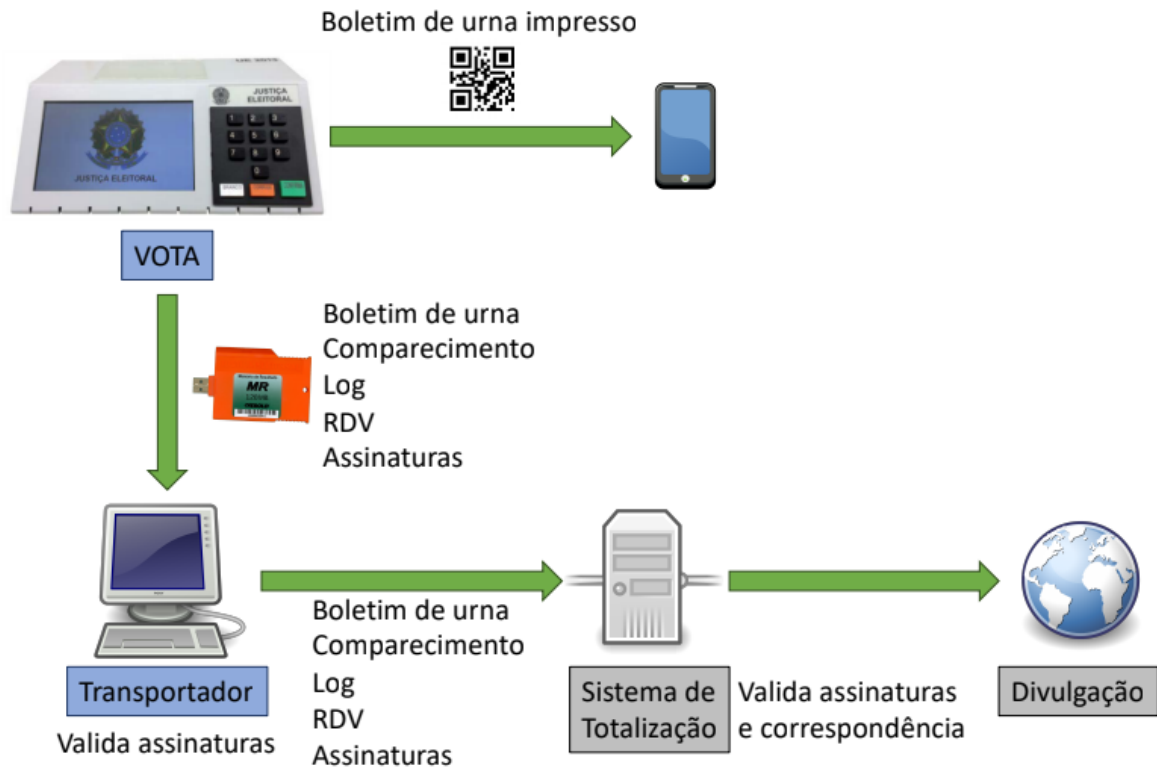
Figura 3: Apuração, Totalização e Divulgação dos resultados.

Fonte: Adaptado de Monteiro et al. (2019)

4 DESAFIOS E SOLUÇÕES EM SISTEMAS DE VOTAÇÃO ELETRÔNICA: UM MAPEAMENTO SISTEMÁTICO

A fim de obter um levantamento de evidências referente aos sistemas de votação eletrônica, foi realizado um Mapeamento Sistemático da Literatura, com o objetivo de descobrir quais são as tecnologias utilizadas nos diferentes tipos de sistemas eleitorais.

É importante destacar que o Mapeamento Sistemático realizado para este estudo foi publicado no IV Workshop de Tecnologia Eleitoral (WTE), evento este que faz parte do Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg)[1], o qual trata-se de um evento cientifico de âmbito nacional promovido anualmente pela Sociedade Brasileira de Computação (SBC). O presente capitulo apresenta a versão estendida do artigo publicado, intitulado *"Desafios e Soluções em Sistemas de Votação Eletrônica: Um Mapeamento Sistemático"* (PEGORINI et al., 2019).

A Seção 4.1 define o que é o Mapeamento Sistemático e a Seção 4.2 apresenta todo o planejamento para a execução do mesmo. Em Seguida, na Seção 4.3 é apresentado os dados da extração e da sintetização dos dados obtidos por meio da execução do mapeamento e a Seção 4.4 trás os resultados alcançados. Por fim, as Seções 4.5, 4.6 e 4.7 apresentam respectivamente, a discussão dos resultados alcançados com o Mapeamento, as ameaças quanto a validade da pesquisa e as considerações finais do referido Capítulo.

4.1 MAPEAMENTO SISTEMÁTICO

Para produzir um conteúdo de qualidade é necessário realizar um levantamento de dados referente ao campo de pesquisa em que se pretende atuar, e para facilitar o agrupamento desses dados, existem diversas técnicas propostas que podem auxiliar todo esse processo. Dentre essas técnicas se encontra o *Mapeamento Sistemático* (MS), que é uma forma de estudo secundário que realiza uma ampla revisão de estudos primários que tenham relação com algum tópico específico, visando identificar evidências sobre o mesmo.

[1]Disponível em: https://sbseg2019.ime.usp.br/

O MS realizado neste estudo se encontra em conformidade com as diretrizes propostas por Kitchenham et al. (2009), que sugeriu que uma prática pioneira nos campos de medicina fosse adotada por pesquisadores da área de Engenharia de Software, propondo uma estrutura de software baseada em evidências. Essa abordagem se baseia em agregar as melhores evidencias disponíveis para abordar uma questão, com base no que outros pesquisadores e profissionais já colocaram sobre o tema. A agregação de todos os estudos empíricos de um determinado tema resulta em uma evidência confiável. Dessa forma as diretrizes médicas foram adaptadas para área da engenharia de software (KITCHENHAM et al., 2010).

O processo do MS envolve três fases principais que são compostas por diferentes atividades. A primeira fase é o planejamento, onde é definido o objetivo e o protocolo, o qual define as questões de pequisa, a estratégia de busca, a seleção das fontes de busca, a *string* de busca, e os critérios de inclusão e exclusão (CI e CE). A segunda fase é a condução, que inicia com a atividade de identificação de estudos primários, seguindo com a seleção desses estudos por meio da aplicação dos CI e CE, e depois a extração e sintetização dos dados. Por ultimo, é realizado a análise dos dados e a divulgação dos resultados (FALBO, 2013).

4.2 PLANEJAMENTO DO MAPEAMENTO SISTEMÁTICO

Na primeira fase do MS é definido um objetivo para a realização do mesmo que, no contexto desse estudo, visa identificar se existem na literatura estudos que abordam quais são os protocolos utilizados em sistemas eleitorais, falhas e vulnerabilidades detectadas, e quais são as medidas de segurança utilizadas por esses sistemas.

4.2.1 QUESTÕES DE PESQUISA

Com o objetivo definido é possível montar uma questão de pesquisa (QP) relacionada ao objetivo, que será utilizada nas atividades seguintes. Levando em consideração que o objetivo desse MS pretendia abordar três assuntos diferentes, foram criadas três QP's diferentes, sendo elas:

- QP_1: Quais os mecanismos ou protocolos utilizados em sistemas de votação eletrônica?
- QP_2: Quais as medidas de segurança utilizadas em sistemas de votação eletrônica?

- QP_3: Quais as vulnerabilidades e falhas públicas detectadas em sistemas de votação eletrônica?

4.2.2 ESTRATÉGIA DE BUSCA E SELEÇÃO

A estratégia de busca do MS define o método de busca utilizado (que se trata de como as buscas pelos estudos serão realizadas), as fontes de pesquisa, a *string* de busca e também a os CI e CE. Depois de todas essas atividades definidas, é possível dar continuidade ao processo do MS.

4.2.2.1 MÉTODO DE BUSCA

Existem três métodos de busca que podem ser utilizadas em MS's:

1. **Busca Automática:** aquela que é feita por meio de bases de dados de estudos indexados;
2. **Busca Manual:** feita por meio de anais e periódicos de eventos realizados na área de pesquisa, quando se tem conhecimento a respeito da realização desses eventos;
3. ***Snowballing*:** é a busca por estudos por meio das referências contidas nos estudos incluídos.

As duas ultimas buscas são buscas complementares à busca automática (FALBO, 2013). Para esse MS, foi utilizada a busca automática pelas bases de dados.

4.2.2.2 FONTES DE BUSCA

Para que seja possível uma cobertura mais abrangente dos trabalhos relacionados, é preciso realizar a busca em mais de uma base de dados. Existem diferentes tipos de bases de dados, onde algumas são bibliotecas digitais de editoras, que são aquelas que contêm basicamente estudos publicados por elas mesmas, e outras bases que são indexadoras, ou seja, bases de dados que indexam estudos de diferentes bibliotecas digitais. Porém, nem todas as bases indexadoras conseguem retornar estudos publicados por algumas bibliotecas digitais, fazendo com que esses estudos sejam retornados apenas por elas mesmas. Por isso é importante realizar a busca tanto nas bibliotecas quanto nas bases indexadoras, para se ter uma melhor cobertura dos estudos (FALBO, 2013).

Neste sentido, as buscas deste MS foram realizadas em quatro bases indexadoras, sendo elas a *Scopus*[2], *Engineering Village*[3], *Springer*[4] e *Sience Direct*[5] e duas bibliotecas digitais, a *ACM Digital Library*[6] e a *IEEE Xplore*[7], de acordo com as diretrizes propostas por Brereton et al. (2007). Além disso, é importante ressaltar que esse procedimento foi conduzido no período de abril a junho de 2019.

4.2.2.3 *STRING* DE BUSCA

Uma *string* de busca tem como objetivo identificar e concatenar os termos chaves da QP, juntamente com os sinônimos de cada um dos termos. Cada termo e seus sinônimos são concatenados com o conectivo OU (do inglês *or*), e cada grupo de termos são concatenados com E, (*AND* em inglês). Para que a *string* de busca seja certeira, é importante que todos os termos estejam alinhados com o tema da pesquisa (FALBO, 2013).

Visando encontrar respostas para as QP's descritas na Subseção 4.2.1, foi necessário criar uma *string* de busca que pudesse responder às três questões definidas. Depois de criada, a *string* precisou ser calibrada para que retornasse resultados precisos, e para isso foi utilizado um conjunto de estudos primários conhecidos como base, apresentados no Quadro 1, chamado de grupo de controle. A calibragem utilizando o grupo de controle consiste em rodar a *string* nas bases de dados, e verificar se os estudos são retornados. Após a calibragem, obteve-se a *string* de busca apresentada no Quadro 2

Quadro 1: Grupo de estudos de controle.

Trabalho	**Título**
Heiderich et al. (2011)	The bug that made me president a browser-and web-security case study on Helios voting
Zhou et al. (2016)	MVP: an efficient anonymous E-voting protocol
Pereira e Wallach (2017)	Clash attacks and the STAR-Vote system
Sebé et al. (2010)	Simple and efficient hash-based verifiable mixing for remote electronic voting

Fonte: Autoria própria.

[2] *www.scopus.com*
[3] *www.engineeringvillage.com*
[4] *https://link.springer.com*
[5] *https://www.sciencedirect.com*
[6] *https://dl.acm.org*
[7] *www.ieeexplore.com*

Quadro 2: *String* de busca construída.

Palavra-chave	**Termos alternativos e/ou sinônimos**
Security	("security" **OR** "secure") **AND**
Threat	("issue" **OR** "breach" **OR** "gap" **OR** "threat") **AND**
E-Voting	("e-voting" **OR** "electronic voting")

Fonte: Autoria própria.

4.2.2.4 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Para garantir a qualidade dos resultados obtidos pelo MS é de suma importância definir alguns critérios de seleção dos estudos, pois esses critérios são responsáveis por estabelecer a relevância de um estudo para o contexto do MS. Os critérios de inclusão e exclusão definem as características que levam à inclusão ou a exclusão de um estudo em específico (FALBO, 2013).

Todos os critérios são definidos levando em consideração as QP's. Dessa forma, para esse MS foram definidos três Critérios de Inclusão (CI), com os quais é possível identificar quais estudos contribuem para as respostas das questões de pesquisa, sendo eles:

- CI_1: estudos primários que apresentam ou propõem uma abordagem, uso ou a aplicação de mecanismos e protocolos utilizados nos sistemas de voto eletrônico;
- CI_2: estudos primários que apresentam ou propõem algum tipo de segurança aplicada a sistemas de votação eletrônica; e
- CI_3: estudos primários que apresentam falhas ou vulnerabilidades detectadas em sistemas de votação eletrônica.

Da mesma forma, os Critérios de Exclusão (CE) também são importantes pois permitem uma maior precisão na eliminação de estudos considerados não relevantes ao contexto da pesquisa em andamento. Por essa razão, durante a análise dos estudos retornados, todos aqueles que enquadraram-se em ao menos um dos sete critérios de exclusão abaixo foram descartados.

- CE_1: estudos primários que mencionam votação em cédulas de papel, ou sistemas de votação que não são eletrônicos;
- CE_2: estudos primários introdutórios para livros;

- CE_3: estudo primários que não sejam *full paper* ou *short paper* (pôsteres, tutoriais, relatório técnicos, teses e dissertações);
- CE_4: estudos primários que seja uma versão anterior de um estudo mais completo sobre a mesma investigação;
- CE_5: estudos primários que não estejam escritos em inglês;
- CE_6: estudos primários em que a versão completa não é disponível; e
- CE_7: estudos primários publicados antes de 2010.

É importante ressaltar que esses critérios são definidos de acordo com as informações que são identificadas e sintetizadas relacionadas à área de pesquisa. Por exemplo, o foco principal do presente estudo refere-se ao uso de sistema eleitorais eletrônicos, dessa forma no critério CE_1 são considerados somente estudos que mencionam esse tipo de sistema eleitoral, visto que protocolos e medidas de segurança aplicados a esses sistemas são diferentes do que aplica-se em sistema de cédulas de papel.

Já o CE_4 foi definido levando em consideração o fato de que informações repetidas de um mesmo estudo pode criar distorções nas conclusões do MS. Muitas vezes acontece de um estudo ser publicado em eventos, e posteriormente ter a sua versão estendida publicada em algum periódico e, nesse caso, considera-se apenas a versão mais recente desse estudo. Porém, para aplicar esse critério, é importante se certificar que o estudo mais recente aborda todo o assunto tratado na versão anterior.

O critério CE_5 foi definido uma vez que o inglês é a língua universal, e tendo em vista que é muito utilizada para a comunidade científica. Assim considerar estudo publicados em utras línguas pode acabar comprometendo os resultados do MS.

Também destaca-se que o CE_7 foi definido levando em consideração as constantes atualizações das tecnologias aplicadas aos sistemas eleitorais, visto que diversos mecanismos e protocolos foram trocados, e medidas de seguranças utilizada foram atualizadas fazendo com que autores publicassem estudos mais recentes sobre estudos mais antigos.

A identificação dos CI e CE compõem a última atividade da primeira etapa do processo do MS.

4.3 CONDUÇÃO DO MAPEAMENTO SISTEMÁTICO

A segunda fase do MS é a condução, que inicia com a atividade de identificação de estudos primários. É importante destacar que os estudos retornados da busca automática podem se repetir entre as bases, pelo fato de estar indexado em mais de uma base de dados, dessa forma a duplicidade de estudos deve ser eliminada antes do processo de seleção dos mesmos (FALBO, 2013).

A seleção dos estudos relevantes se dá por meio de etapas que utilizam filtros de leitura para auxiliar no processo de seleção, e para isso são aplicados três filtros de leitura:

1. Leitura de título e *abstract*;
2. Leitura da introdução e conclusão; e
3. Leitura do estudo na íntegra.

Destaca-se que, em todos os filtros de leitura, devem ser aplicados os CI e CE para cada estudo analisado.

Com a execução da *string* de busca nas bases de dados, obteve-se um total de 2117 estudos, dos quais 164 foram excluídos por se tratar de estudos duplicados. A Tabela 1 apresenta a relação dos estudos retornados por cada umas das bases utilizadas.

Tabela 1: Quantidade de estudos retornados por base de dados eletrônica.

Base de Dados	Quantidade
ACM Digital Library	49
Elsevier (via Science Direct)	767
Engineering Village	129
IEEE Xplore	47
Springer	840
Scopus	285
Total	**2117**

Fonte: Pegorini et al. (2019).

Na primeira etapa do processo de seleção, com a leitura do título e *abstract* dos estudos restantes (1953), foram excluídos 1490 estudos pois se mostraram irrelevantes ao tema abordado. Seguindo para a segunda etapa, a análise da introdução e conclusão, foram excluídos mais 372 dos 463 estudos que passaram pela primeira etapa, restando apenas 91 para a terceira etapa e aplicação do terceiro filtro, onde a leitura na íntegra excluiu 47

estudos que não se encaixavam nos CI's e CE's, totalizando 44 estudos relevantes incluídos por essa seleção final. A Figura 4 apresenta uma visão geral desse processo de condução do MS.
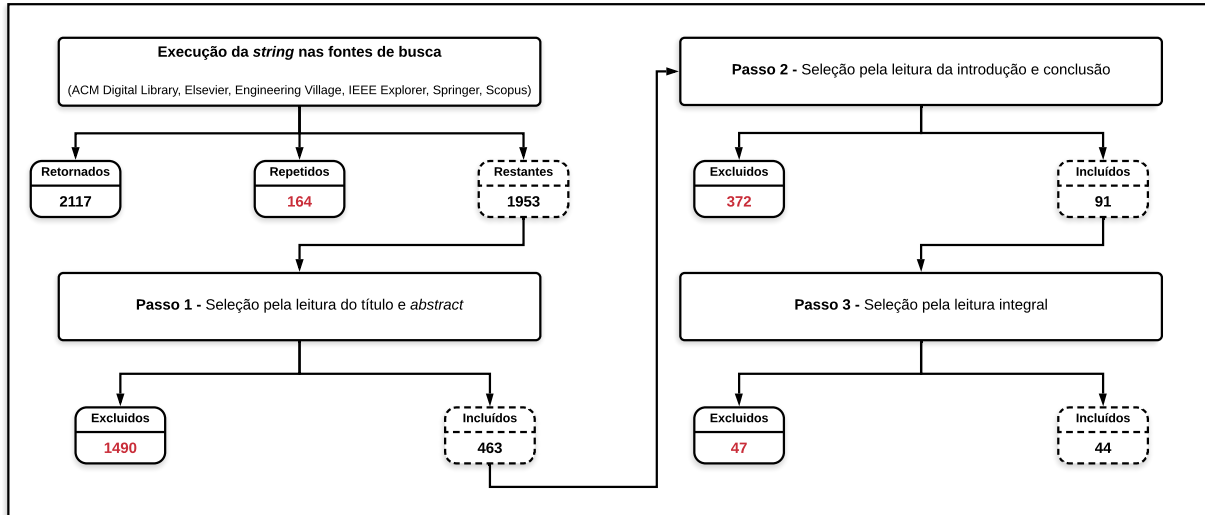
Figura 4: Condução do Mapeamento Sistemático.
Fonte: Pegorini et al. (2019).

4.3.1 EXTRAÇÃO E SINTETIZAÇÃO DOS DADOS

Depois de concluído a seleção final dos estudos, deu-se início a extração dos dados de cada um dos 44 estudos, os quais foram incluídos por serem considerados relevantes ao tema. Eles abordavam diretamente assuntos que respondiam às QP's definidas anteriormente. A partir da extração dos dados de cada estudo primário, foi possível organizá-los em três categorias de acordo com os assuntos que cada um deles aborda, sendo elas :

- C_1: **Protocolos:** reúne estudos que abordam algum tipo de protocolo de segurança utilizado em sistemas eleitorais;
- C_2: **Medidas de Segurança:** contém os estudos relacionados à medidas de segurança aplicados ao sistemas de votação eletrônica; e
- C_3: **Falhas e Vulnerabilidades:** consiste na seleção dos estudos que apresentam as vulnerabilidades e falhas detectadas em sistemas eletrônicos de votação.

Diante dessas categorias, foram classificado três objetivos principais abordados diretamente por alguns dos estudos incluídos. Esses objetivos são:

- O_1: **Identificação:** engloba a identificação de vulnerabilidades e falhas detectadas em sistemas de votação, medidas de segurança aplicadas aos protocolos já existentes que são utilizados nesses sistemas, e também propõe alguns novos protocolos que implementam medidas de segurança já existentes;
- O_2: **Melhoria:** estudos que propõem melhorias em protocolos ou medidas de segurança aplicadas a sistemas de votação; e
- O_3: **Mitigação:** estudos que abordam formas de aliviar ou suavizar as vulnerabilidades em sistemas de votação.

Após realizar a leitura integral dos estudos, foi possível fazer uma associação de uma ou mais categorias abordadas em cada um dos estudos, conforme será descrito na Seção 4.4.

4.4 ANÁLISE DOS RESULTADOS

A última etapa do processo de MS é a análise dos principais dados de cada um dos 44 estudos incluídos, que contemplam dados como o ano e tipo de publicação, país de origem do autor (considerando o primeiro autor), classificação dos estudos pelas categorias e objetivos especificados na Seção 4.3.1, entre outros dados considerados importantes.

Na Figura 5, é apresentado a visão geral dos estudos primários publicados por ano. É possível observar que entre os estudos incluídos, o ano em que concentra-se o maior número de estudos dentre os selecionados, é o ano de 2015, contendo 9 estudos publicados. Já nos anos de 2012 e 2014 não foi selecionado nenhum estudo.
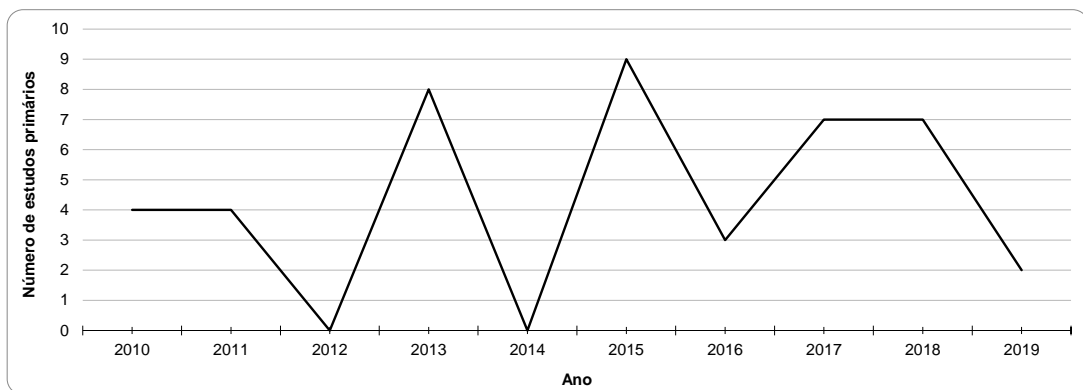
Figura 5: Relação de estudos por ano de publicação.

Fonte: Pegorini et al. (2019).

Os estudos também foram analisados em relação ao país de origem do autor principal, conforme apresentado na Figura 6, onde é possível observar que os países com o maior índice de estudos publicados são a Índia e a China, com 6 e 4 estudos respectivamente. Em seguida encontram-se a Coreia do Sul e a Espanha com 3 estudos cada.
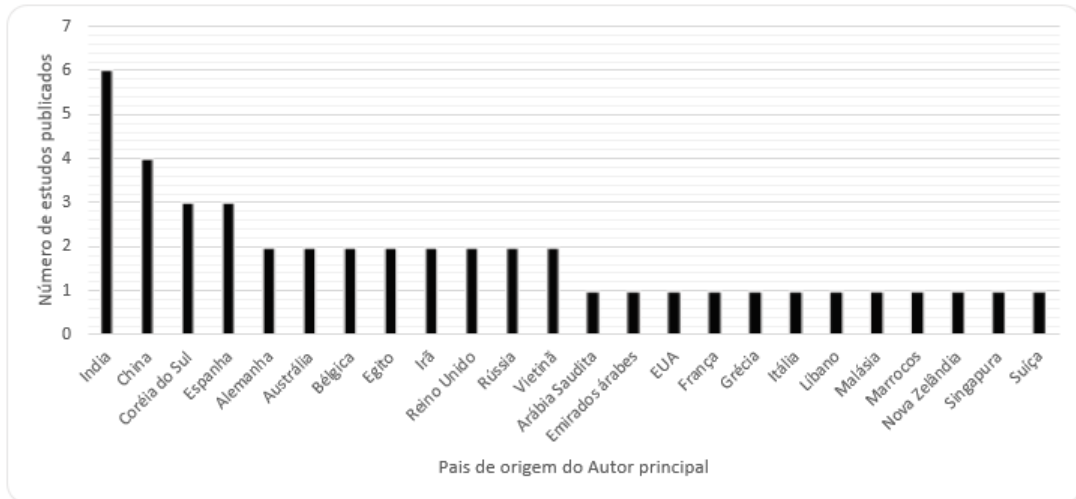
Figura 6: Relação de estudos por país de origem do autor principal. Fonte: Adaptado de Pegorini et al. (2019).

Levando em consideração que estudos científicos são publicados e divulgados em diferentes tipos de eventos, 39% dos 44 incluídos foram publicados em periódicos, o que representa um total de 17 estudos. Os outros 27 que representam 61%, foram publicados em conferências, conforme apresentado na Figura 7.
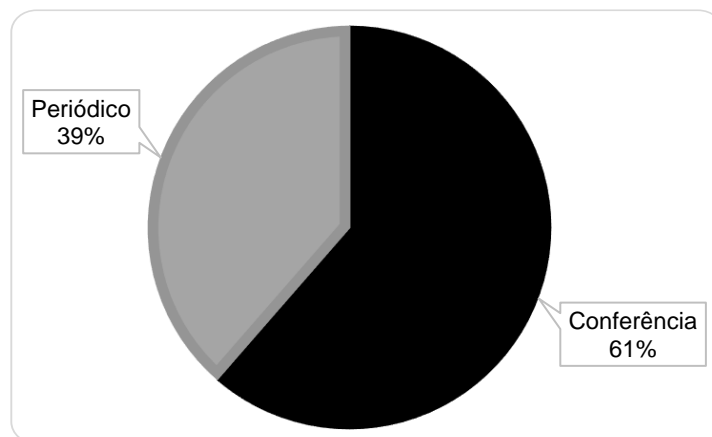
Figura 7: Relação de estudos por ano tipo publicação. Fonte: Pegorini et al. (2019).

Destaca-se que 10 desses estudos foram publicados em eventos realizados no país

de origem do autor principal, o que representa 37% dos 27 estudos. Foi possível observar ainda que outros 2 estudos foram publicados em eventos que ocorreram no país de origem de pelo menos um dos autores, correspondendo à 7,4% dos estudos.

Um forte indicativo da relevância de um estudo é o numero de vezes que o mesmo foi citado por outros autores. Dessa forma, a Figura 8 apresenta a relação dos estudos mais citados dentre os estudos incluídos durante o processo do MS. O número de citações de cada estudo foi coletadas pelo *Google Scholar*.
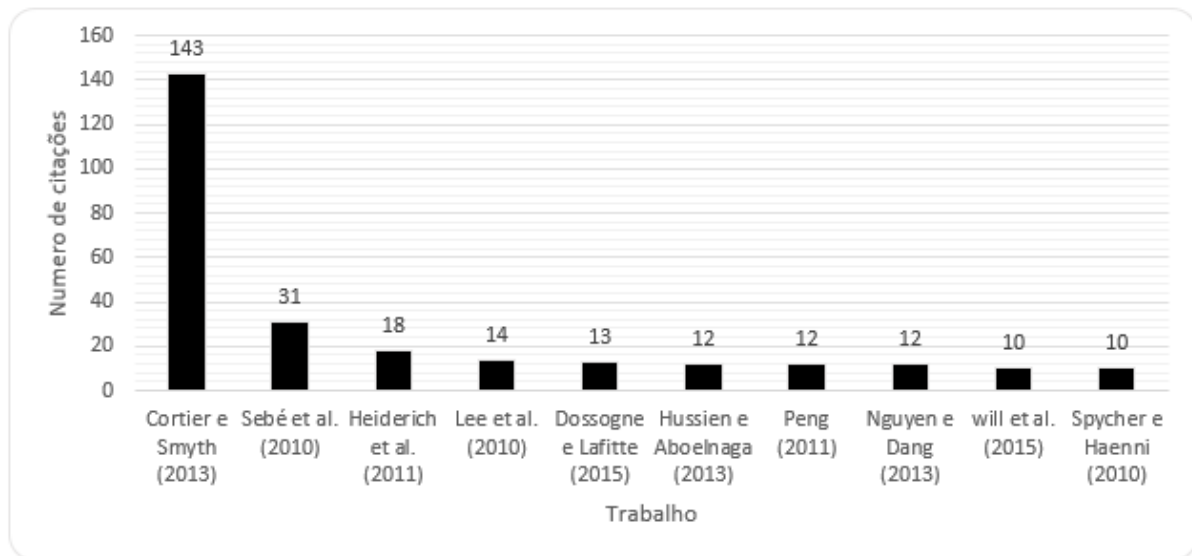
Figura 8: Relação de estudos por número de citações.
Fonte: Autoria própria.

De acordo com as categorias citadas na Subseção 4.3.1, a Figura 9 apresenta o número de estudos que se enquadram em cada uma das categorias e as suas respectivas interseções. Dentre os 44 estudos incluídos, nenhum deles está relacionado somente à C_1, diferente de C_2 e C_3 que apresentaram 11 e 2 estudos, respectivamente. Notou-se que nas interseções entre C_1 e C_2, C_2 e C_3 e C_1 e C_3, foram encontrados respectivamente, 15, 9 e 0 estudos. Já na interseção das três categorias, foram encontrados 7 estudos.

Como discutido anteriormente, alguns estudos puderam ser classificados em mais de uma categoria, uma vez que os autores relacionavam a existência de um protocolo específico para uma medida de segurança implementada em um sistema de votação, ou algum tipo de vulnerabilidade ou falha de algum protocolo ou medida de segurança proposta.

Na Figura 10 é ilustrado o mapeamento dos estudos relacionando os objetivos
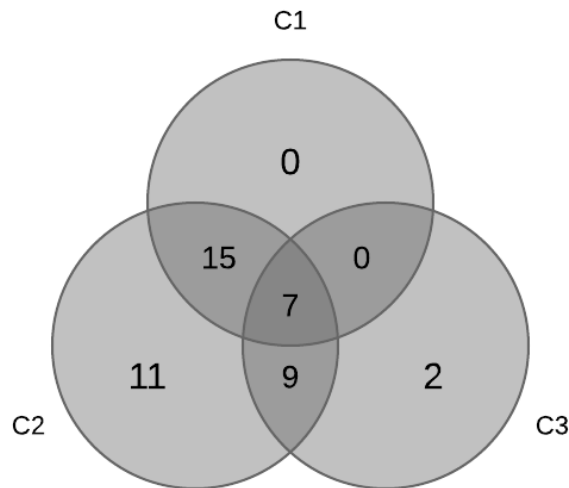
Figura 9: Interseção de estudos por categorias.

Fonte: Pegorini et al. (2019).

com as categorias. Os estudos foram organizados da seguinte forma: no eixo x estão os três objetivos identificados na Seção 4.2.2.4, e no eixo y estão as categorias. Os valores que aparecem nas interseções entre os eixos x e y representam o número de estudos que citam o(s) objetivo(s) que foram relacionados a uma determinada categoria. O tamanho de cada circunferência (*bubble*) é representado pelo número de estudos classificados em ambos os pares de categorias.
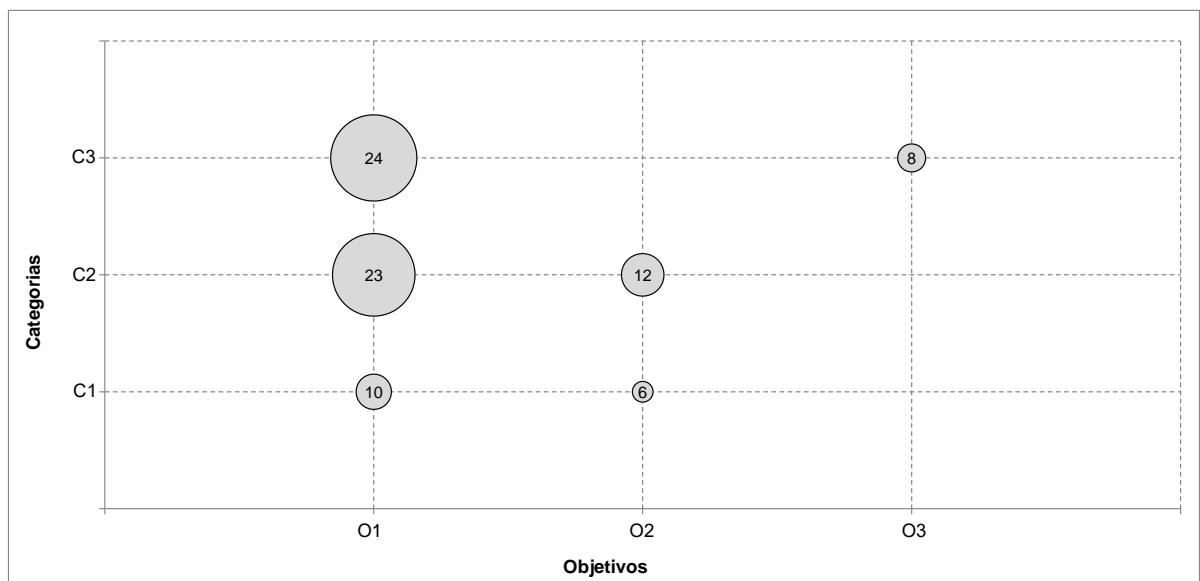
Figura 10: Classificação de estudos por categorias e objetivos.

Fonte: Pegorini et al. (2019).

Dentre os 44 estudos incluídos, apenas 10 abordaram a proposta (O_1) de um novo protocolo (C_1), e 6 propuseram melhorias (O_2) em protocolos (C_1) já existentes. Em segundo plano observa-se que 23 estudos identificaram (O_1) o funcionamento de algum tipo de medida de segurança (C_2) existente, enquanto que em 12 desses estudos foram propostas melhorias (O_2) para medidas de segurança (C_2) existentes. Nas falhas e vulnerabilidades (C_3) identificadas (O_1), foram encontrados um total de 24 estudos, com somente 8 apresentando a mitigação (O_3) dessa categoria (C_3). A classificação e categorização integral de todos os estudos analisados pode ser conferida no Quadro 3.

4.5 DISCUSSÃO

Muitas ameaças rondam a segurança de um sistema computacional, podendo colocar em risco os recursos do mesmo. Uma ameaça é um evento que se aproveita de falhas de segurança e explora uma falha específica, podendo resultar em uma vulnerabilidade que causa brechas de segurança do sistema. Muitos países vêm gradativamente substituindo seu tradicional sistema de votação em papel para sistemas eletrônicos, os quais podem ser encontrados em duas categorias diferentes: *Votação eletrônica supervisionada*, que trata-se da votação perante as autoridades eleitorais em locais específicos para realização de eleições, e faz utilização de urnas eletrônicas físicas para a coleta dos votos, e a *Votação Eletrônica Remota*, que é de exclusiva responsabilidade do eleitor, tendo em vista que ela não é supervisionada fisicamente por nenhum tipo de autoridade governamental. Um exemplo desse tipo de votação, é a votação pela Internet (ZISSIS; LEKKAS, 2011).

Levando em consideração os estudos retornados pelo MS, pode-se observar que existem diversos protocolos utilizados em sistemas de votação eletrônica, onde cada qual possui um objetivo diferente com a finalidade de garantir que o sistema implemente as principais propriedades de segurança. Porém, alguns protocolos acabam sofrendo com algum tipo de falha, ocasionando uma vulnerabilidade no sistema. Um exemplo disso, é o protocolo de contagem de votos de Nassar, Malluhi e Khan (2018), que por meio de um ataque de negação de serviço, ou ataque DoS, faz com que seu servidor de contagem de votos não seja confiável. Outro exemplo é o protocolo TPKE, pois é suscetível ao ataque MITM podendo causar a perda de privacidade do eleitor (KIAYIAS; ZACHARIAS; ZHANG, 2017; KIAYIAS; ZACHARIAS; ZHANG, 2015).

Quadro 3: Quadro geral da classificação dos estudos incluídos.

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Jin et al. (2019)	Protocolo de Autenticação negável Heterogênea HDA	Autenticação Verificação em Lote	-	-	Remota
Gurubasavanna et al. (2018)	-	Autenticação Biométrica Captura de Face	-	-	Supervisionada
Bistarelli et al. (2019)	-	Bitcoin Multchain	-	-	Remota
Nassar, Malluhi e Khan (2018)	Protocolo de Contagem de Votos	Criptografia Homomórfica de Paillier	Negação de Serviço	Servidor de Contagem de votos não confiável Intromissão da Rede	Remota
Babenko e Pisarev (2018)	Protocolo Descrito na Linguagem CAS+	Autenticação das partes Sigilo de Dados Proteção contra ataques de repetição	-	-	Supervisionada

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Saqib et al. (2018)	Protocolo baseado em Assinatura Cega	Biometria	-	-	Remota
Yu et al. (2018)	-	Blockchain Criptografia Homomórfica	-	-	Remota
Zhu, Zeng e Lv (2018)	-	Blockchain Assinatura Cega Assinatura de Anel	-	-	Remota
Lakshmi e Kalpana (2018)	-	Identificação Exclusiva (AADHAR) Biometria	-	-	Supervisionada
Haines e Boyen (2016)	Prêt à Voter	Criptografia Híbrida Recriptografia	Produção de recibo com assinatura falsa	-	Remota
Pereira e Wallach (2017)	-	Verificação Ponta-a-Ponta	Modificação do *hash* dos votos	Ataque de choque em máquinas trapaceiras	Supervisionada

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Hsiao et al. (2017)	-	Criptografia de Curva Elíptica Criptografia Assimétrica Função *hash* Assinatura de Anel	-	-	Remota
AboSamra et al. (2017)	Protocolo baseado no conceito do Prêt à Voter	Criptografia de Chave Simétrica Criptografia de Chave Pública	-	-	Supervisionada
Kate e Katti (2016)	-	Algoritmo de Criptografia AES Criptografia Visual	-	-	Remota
Kumar, Katti e Saxena (2017)	Protocolo ID-BS	Assinatura Cega de Bodyreva Assinatura Baseada em Identidade de Chon-Cheon	-	-	Remota

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Shakiba, Doostari e Mohammadpourfard (2017)	Protocolo ESIV	JavaCard 3	-	-	Remota
		Criptografia de Chave Pública			
Kiayias, Zacharias e Zhang (2017)	TPKE	Esquema de Compartilhamento Secreto Verificável	Quebra da privacidade do eleitor	Sucetível ao ataque MITM	Remota
Babenko, Pisarev e Makarevich (2017)	-	Criptografia Simétrica	Qualquer pessoa pode votar	Vulnerabilidade humana	Supervisionada
		Gost		Influenciar legalmente o resultado das eleições	
		Função *hash*		Identificação do usuário	
Zhou et al. (2016)	MVP	DRMM	-	-	Remota
Chang et al. (2015)	Apollo	Criptografia de Chave Assimétrica	-	Perda da privacidade do eleitor	Remota
		Criptografia de Chave Simétrica			

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Will et al. (2015)	-	Criptografia Homomórfica Agentes Móveis	-	Agentes móveis não são tão robustos quanto as exigências do governo	Remota
Dossogne e Lafitte (2015)	Protocolo de Auto-Cálculo	Criptografia de Chave Pública Homomórfica Criptografia de Paillier Criptografia ElGamal	-	-	Remota
Zhang, You e Zhang (2015)	Kerberos	Criptografia de Chave Simétrica Assinatura Cega	Negação de serviço	-	Remota
Tornos, Salazar e Piles (2015)	Protocolo de Votação Portátil	Criptografia de Anel Criptografia de Chave Pública PKB	-	-	Remota
Kiayias, Zacharias e Zhang (2015)	TPKE	Criptografia de Chave Pública Benaloh Challenge	-	Sucetível ao ataque MITM	Remota

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Mohammadpourfard et al. (2015)	FOO	Criptografia RSA	-	-	Remota
		JavaCard 3			
Rura, Issac e Haldar (2015)	-	Criptografia Visual	Ataque DoS	Incoercibilidade	Remota
		Sistema Criptográfico de Decriptação	Ataque de abstenção forçada		
		Esteganografia			
Kartit et al. (2015)	-	Criptografia ElGamal	-	-	Remota
		Criptografia Homomórfica RSA			
Huarte et al. (2013)	Protocolo do Canal Anônimo	Criptografia Cega	-	-	Remota
		SmartCards			
		Inspeção NVP			
		Proteção a Prova de Voto			
Srinivasan et al. (2013)	TPKE	TCE - Criptografia Controlada por Token	Ataque de enchimento de células	-	Remota

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Kim et al. (2013)	-	Assinatura Cega Criptografia Independente Compartilhamento Secreto	-	-	Remota
Hussien e Aboelnaga (2013)	-	Assinatura Cega Baseada em RSA Criptografia Homomórfica	-	-	Remota
Khelifi et al. (2013)	-	Assinatura Cega Assinatura de Anel Comprometimento de Bits	Falhas humanas	-	Remota
Nguyen e Dang (2013b)	Protocolo Livre de Colusão	Assinatura Cega Criptossistema de Chave Simétrica	-	-	Remota

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Nguyen e Dang (2013a)	Protocolo de Votação pela Internet	Assinatura Cega	Falhas humanas	-	Remota
		Células Dinâmicas			
		Criptossistema de Chave Simétrica			
Heiderich et al. (2011)	-	-	Invasor interfere em um processo de votação sem deixar rastros	Controle remoto de localização	Remota
			Extração de dados via CSS	Não utiliza cabeçalho HTTP	
Olembo, Schmidt e Volkamer (2011)	-	Autenticação Baseada em Segredo	-	Software mal-intencionado	Remota
		Token de Autenticação			
Cortier e Smyth (2013)	-	Remoção de Células Duplicadas	Helios permite que o voto do eleitor seja revelado	-	Remota

Continua na próxima página

Quadro 3 – *Continuação da página anterior*

Estudos primários	**QP_1: Protocolo**	**QP_2: Medidas de Segurança**	**QP_3**		**Votação Eletrônica**
			Falhas	**Vulnerabilidades**	
Lavanya (2011)	-	-	Ataque de roubo de votos	-	Supervisionada
			Ataque DoS		
Peng (2011)	-	Criptografia de Rede Mista	Ataque de relação em rede mista	-	Remota
Lee et al. (2010)	-	Autenticação	-	Mal funcionamento	Remota
		Encriptação		Alteração no registro de votação	
		Auditoria		Votação não autorizada	
				Alteração de dados do sistema	
Yoon et al. (2010)	Protocolo de Autenticação Confiável	Criptografia ElGamal	-	-	Remota
Sebé et al. (2010)	-	Criptografia ElGamal	-	-	Remota
Spycher e Haenni (2010)	Protocolo de Sistema Híbrido	Criptografia ElGamal	-	-	Remota
		Criptografia Limiar			

Fonte: Adaptado de Pegorini et al. (2019).

Uma das medidas de segurança aplicadas ao TPKE é a baseada em criptografia de chaves públicas, como mostra o estudo de Kiayias, Zacharias e Zhang (2015). Entretanto, diferentes outros tipos de protocolos, como o baseado no conceito do *Pret-à-voter* (ABOSAMRA et al., 2017), protocolo ESIV (SHAKIBA; DOOSTARI; MOHAMMAD-POURFARD, 2017), e protocolo de auto-cálculo (DOSSOGNE; LAFITTE, 2015) também utilizam esse tipo de medida de segurança, onde a criptografia de ElGamal também é utilizada no protocolo de Auto-Cálculo. Os protocolos de autenticação confiável (YOON et al., 2010), e protocolo de sistema híbrido (SPYCHER; HAENNI, 2010) também utilizam essa criptografia em seu sistema de segurança.

A assinatura cega é uma das medidas de segurança mais utilizadas pelos autores em diferentes sistemas e tipos de protocolos (ZHU; ZENG; LV, 2018; KUMAR; KATTI; SAXENA, 2017; ZHANG; YOU; ZHANG, 2015; HUARTE et al., 2013; KIM et al., 2013; KHELIFI et al., 2013; NGUYEN; DANG, 2013b; NGUYEN; DANG, 2013a), onde combinada com outras medidas de segurança podem garantir o anonimato do eleitor e a segurança do sistema. Nesse sentido, ela é utilizada para evitar uma das ameaças mais comuns desse tipo de sistema, o ataque de negação de serviço (NASSAR; MALLUHI; KHAN, 2018; ZHANG; YOU; ZHANG, 2015; RURA; ISSAC; HALDAR, 2015; LAVANYA, 2011). Além da assinatura cega, a criptografia homomórfica de Paillier (NASSAR; MALLUHI; KHAN, 2018), criptografia de chave simétrica (ZHANG; YOU; ZHANG, 2015), criptografia visual, decriptação e esteganografia (YU et al., 2018) também são técnicas de segurança utilizadas para evitar esse tipo de ataque.

Entre os sistemas de votação, o que mais teve destaque negativo foi o Hélios, que se trata de um sistema de votação pela Internet. Estudos como os de Kiayias, Zacharias e Zhang (2017) e Srinivasan et al. (2013) mostram que esse sistema é suscetível ao ataque MITM e ataque de enchimento de cédulas, podendo sofrer também de uma vulnerabilidade que pode revelar o voto do eleitor (KIAYIAS; ZACHARIAS; ZHANG, 2017; CORTIER; SMYTH, 2013). Além disso o estudo de Heiderich et al. (2011) mostra que esse sistema não implementa o cabeçalho HTTP. As medidas de segurança aplicadas a esse sistema se tratam de esquemas de compartilhamento secreto verificável, criptografia controlada por *token* e remoção de cédulas replicadas.

4.6 AMEAÇAS À VALIDADE

Alguns tipos de ameaças quanto a validade da pesquisa são definidas em Wohlin et al. (2012). Dessa forma, neste MS foram identificadas as seguintes ameaças à validade:

- **Validade de Conclusão:** esse tipo de validade esta ligado a relação entre o tratamento e os resultados de uma forma estatística, dessa forma, vale destacar a criação e adaptação da *string* de busca. Como as palavras e expressões que a compõem são derivadas das QP's, a correta construção dessa é vital para a efetividade da pesquisa. Para mitigar esta ameaça, a *string* de busca foi criada e calibrada para verificar se os estudos definidos como controle, na Seção 4.2.2, retornaram com a *string* de busca executada. Além disso, foi solicitado a um profissional da área que avaliasse a *string* para validá-la e melhorar sua efetividade.

- **Validade Interna:** Wohlin et al. (2012) descrevem esse tipo de ameaça à validade como a relação casual entre o tratamento e os resultados. Nesse sentido, essa ameaça é observada diante a indisponibilidade de acesso a alguns estudos retornados pela *string* de busca, não sendo possível a inclusão do mesmo ao processo de condução do MS.

- **Validade de Construção:** Para Wohlin et al. (2012) esse tipo de ameaça está ligada a relação entre a teoria e a prática, dessa forma, no contexto do MS a ameça está relacionada ao processo de seleção de estudos. Para minimizar essa ameaça, com o objetivo de assegurar um processo de seleção imparcial e evitar vieses foi desenvolvido um protocolo de pesquisa sobre as orientações estabelecidas por Kitchenham et al. (2010). Esse protocolo contém as questões de pesquisa, estratégia de busca, critérios de inclusão e exclusão, bem como a forma como os dados serão extraídos.

- **Validade Externa:** Essa ameaça refere-se a generalização dos resultados em campo externo ao estudo Wohlin et al. (2012). Sendo assim, a ameaça diz respeito à possibilidade de publicações de estudos relevantes em plataformas não indexadas, os quais não são retornados pela busca automática realizada neste MS.

4.7 CONSIDERAÇÕES FINAIS

O presente capítulo apresentou e discutiu os resultados de um MS conduzido com o objetivo de identificar os principais protocolos de votação eletrônica utilizados, as vulnerabilidades e falhas em que esses sistemas são expostos, além das medidas de segurança mais utilizadas por esses sistemas.

É importante destacar que um MS é suscetível a falhas, especialmente quando a identificação dos estudos primários é feita somente por buscas automatizadas em bases de dados indexados. Em geral, o MSto contribuiu para um melhor entendimento do atual

estado da arte dos sistemas eleitorais para a identificação de limitações, protocolos e medidas de segurança usados, além das vulnerabilidades que esses sistemas sofrem.

Os resultados mostraram um grande número de estudos que discutem sobre as falhas encontradas em protocolos utilizados por diferentes sistemas eleitorais em todo o mundo, e também as várias medidas de segurança que podem ser implementadas por esses tipos de sistemas, para garantir que as ameaças à segurança dos mesmos seja amenizada.

5 TESTES PÚBLICOS DE SEGURANÇA: UM ESTUDO DE CASO

Os anos que antecedem uma eleição são marcados por um evento promovido pela Justiça Eleitoral, o qual reúne diversos especialistas das mais variadas instituições, que se dirigem à sede do TSE em Brasília-DF para participar do Teste Público de Segurança (TPS). Na ocasião o sistema eleitoral brasileiro é disposto aos profissionais, que podem realizar planos de ataque contra os ecanismos de segurança do mesmo, na tentativa de quebra-lo. A primeira edição do evento ocorreu em 2009 e após isso outras três edições foram realizadas. A Figura 11 mostra a representação dos principais resultados alcançados pelos investigadores durante as quatro edições do TPS, realizadas até a edição de 2017.
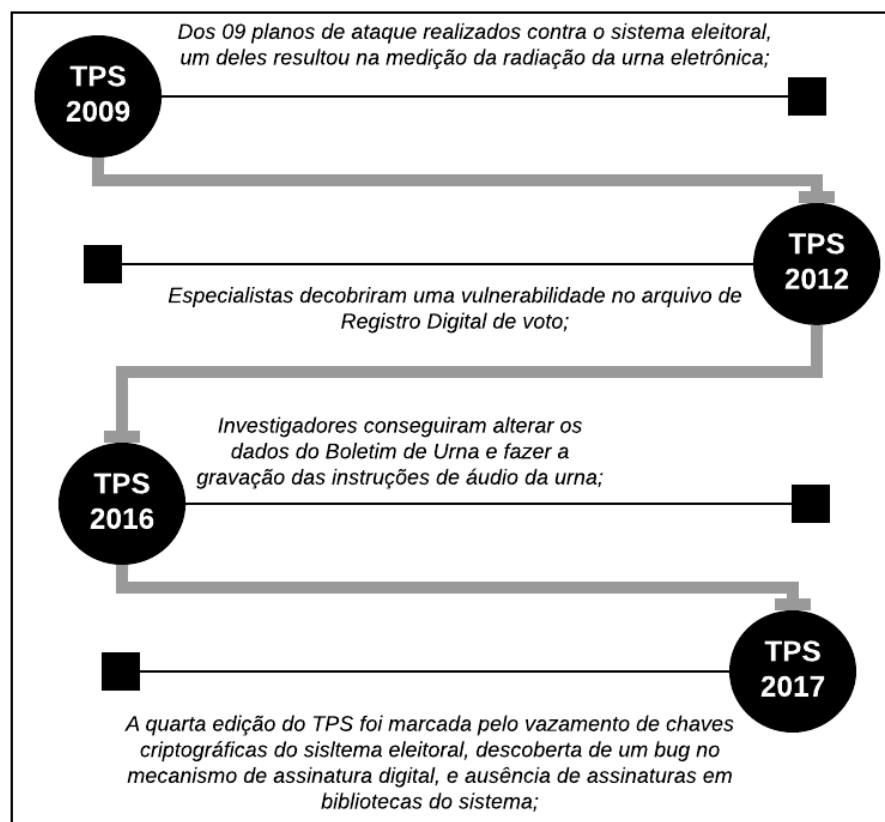
Figura 11: Linha do tempo do TPS.

Fonte: Autoria Própria

Este Capítulo apresenta as principais informações sobre esse evento e as edições já realizadas. Além disso é realizado um estudo de caso sobre os resultados alcançados pelos investigadores que participaram das quatro edições do evento realizados até o momento, fazendo uma análise comparativa entre cada uma das edições. O levantamento das informações necessárias se deu por meio do estudo da documentação apresentada pela Justiça Eleitoral, documentação essa que continha os relatórios públicos de avaliação dos TPSs disponibilizados pela mesma.

Dessa forma, a Seção seguinte, 5.1 descreve o TPS e apresenta as informações de cada uma das edições já realizadas. Em seguida, a Seção 5.2 apresenta o protocolo de estudo de caso seguido para a realização do mesmo, o qual segue a proposta de Wohlin e Aurum (2015). Na Seção 5.3 é apresentado o levantamento das informações colhidas pela documentação analisada, apresentando os principais resultados sobre os planos de ataque executados contra o sistema eleitoral. Por fim, nas Seções 5.4 e 5.5 são apresentadas as ameaças à validade da pesquisa desenvolvida, e as considerações finais sobre o Capítulo, respectivamente.

5.1 TESTE PÚBLICO DE SEGURANÇA

O TPS é um evento permanente da Justiça Eleitoral Brasileira, criado com o intuito de aprimorar o processo eletrônico de votação. Esse evento conta com a participação e colaboração de especialistas que buscam por problemas ou fragilidades nas urnas eletrônicas, e uma vez que tais problemas são detectados, são resolvidos e testados.

Na primeira edição do TPS realizada em 2009, os investigadores não obtiveram sucesso nos testes realizados. No entanto, suas ideias contribuíram para o aperfeiçoamento tecnológico da votação. Em contrapartida, no ano de 2012 durante a segunda edição do evento os investigadores participaram da fase de preparação e tiveram acesso ao código-fonte da urna eletrônica para que pudessem se inteirar ainda mais das peculiaridades do sistema e realizar seus planos de ataque (Tribunal Superior Eleitoral, 2019b).

Apesar do sucesso dessas duas primeiras edições o TSE recebeu diversas críticas e sugestões quanto à metodologia utilizada pelo mesmo na avaliação dos trabalhos desenvolvidos pelos investigadores que participaram das edições anteriores, optando pela não realização do evento no ano de 2014. A decisão foi tomada a fim de fazer uma revisão da metodologia de avaliação utilizada como um todo para os eventos seguintes (ADAMEK et al., 2016).

De volta com o evento no ano de 2016, os participantes da terceira edição apresentaram previamente os seus planos de ataque, e assim puderam ter acesso aos componentes internos e externos do sistema eletrônico de votação. Finalmente, na última edição realizada no ano de 2017 foram executados 10 planos de teste, dentre os quais 4 contribuíram para o aprimoramento do processo eleitoral. No ano de 2019 o evento ocorre entre os dias 25 a 29 de novembro (Tribunal Superior Eleitoral, 2019b).

Para participar do TPS os interessados precisam se inscrever de forma individual ou em grupo por meio de editais disponibilizados pela Justiça Eleitoral, onde constam todas as informações acerca da realização do mesmo. Para a inscrição os interessados devem encaminhar previamente seus planos de ataque e, se aprovados pela Justiça Eleitoral, se dirigirem até Brasília na sede no TSE para a realização dos mesmos nas datas estipuladas (Justiça Eleitoral, 2019).

Segundo a Justiça Eleitoral, o TPS é realizado seguindo três etapas que envolvem a preparação, a realização e a avaliação do evento. A fase de preparação é a etapa em que são recebidas as pré-inscrições, inscrições, planos de ataque, apresentação dos sistemas e códigos fontes e demais atividades que antecedem o evento. Em seguida, na fase de realização, os investigadores inscritos em tempo do edital comparecem ao local onde os testes são realizados e colocam previamente em prática os seus planos de ataque. Por fim, a comissão avaliadora realiza a análise dos relatórios de teste de cada investigador, ou grupo, e produz o relatório final apresentando todos os resultados alcançados (Justiça Eleitoral, 2019).

Para cada edição do evento, e para que o TPS seja realizado com sucesso, são montadas quatro comissões de apoio compostas por membros de diferentes áreas do TSE. A comissão organizadora se responsabiliza em planejar e elaborar o projeto geral das atividades, por ouro lado, a comissão reguladora é responsável por definir os procedimentos e a metodologia do processo e também supervisar as etapas do mesmo. A terceira comissão é a avaliadora, a qual avalia e valida a metodologia e os critérios de julgamento, além de homologar e avaliar os resultados. Essa comissão conta com representantes da comunidade acadêmica e cientifica, Ministério Público Federal (MPF), Ordem dos Advogados do Brasil (OAB), Congresso Federal e Sociedade Brasileira de Computação (SBC). Além disso, também participa dessa comissão um representante do TSE e um um engenheiro eletricista/eletrônico ou de computação devidamente registrado no Conselho Regional de Engenharia e Agronomia (CREA) indicado pelo Conselho Federal de Engenharia e Agronomia (CONFEA). A quarta e última comissão é a Comunicação Institucional, que

é responsável pela divulgação do TPS e por responder questionamentos do público e da imprensa.

Como mencionado anteriormente, o TPS reúne especialistas em Tecnologia e Segurança da Informação de diversas organizações para executar planos de ataque contra o Sistema Eleitoral Brasileiro, com a intenção de identificar eventuais falhas e vulnerabilidades nos procedimentos ou nos sistemas de computação e, para que a partir dos resultados alcançados, seja possível a melhoria e aprimoramento do sistema. O TPS também tem o intuito de testar a confiabilidade da captação e apuração dos votos verificando a robustez e a maturidade do sistema, de forma a realizar melhorias constantes no processo como um todo (Justiça Eleitoral, 2019).

5.2 ESTUDO DE CASO

Quando uma pesquisa é realizada com intuito investigar determinado assunto, existem métodos que podem ser utilizados para auxiliar o desenvolvimento da mesma, e um desses métodos é o estudo de caso.

Essa estratégia tem o propósito de reunir informações sistemáticas sobre um fenômeno, que se concentra na compreensão de um contexto real por meio de um estudo aprofundado sobre o mesmo, de maneira que se obtenha o maior detalhamento possível sobre o contexto estudado. O estudo de caso é elaborado a partir de múltiplas fontes de prova que podem incluir dados de diversas formas de levantamento de evidências, sustentado por um referencial teórico que orienta as questões e preposições do estudo (FREITAS; JABBOUR, 2011).

Dessa maneira, no presente capítulo é apresentado o estudo de caso realizado com base em pesquisa de arquivos públicos sobre os resultados alcançados por investigadores de múltiplas instituições, que participaram das quatro edições dos TPSs realizados até o momento, a fim de explicar as fases desse processo e comparar os resultados alcançados por esses pesquisadores.

5.2.1 PROTOCOLO DO ESTUDO DE CASO

O presente estudo de caso segue o protocolo proposto por Wohlin e Aurum (2015), onde a Figura 12 apresenta a ilustração das fases de tomada de decisão de uma pesquisa científica. Tal protocolo segue uma estrutura de decisões que se divide três fases: Estratégica, Tática e Operacional.
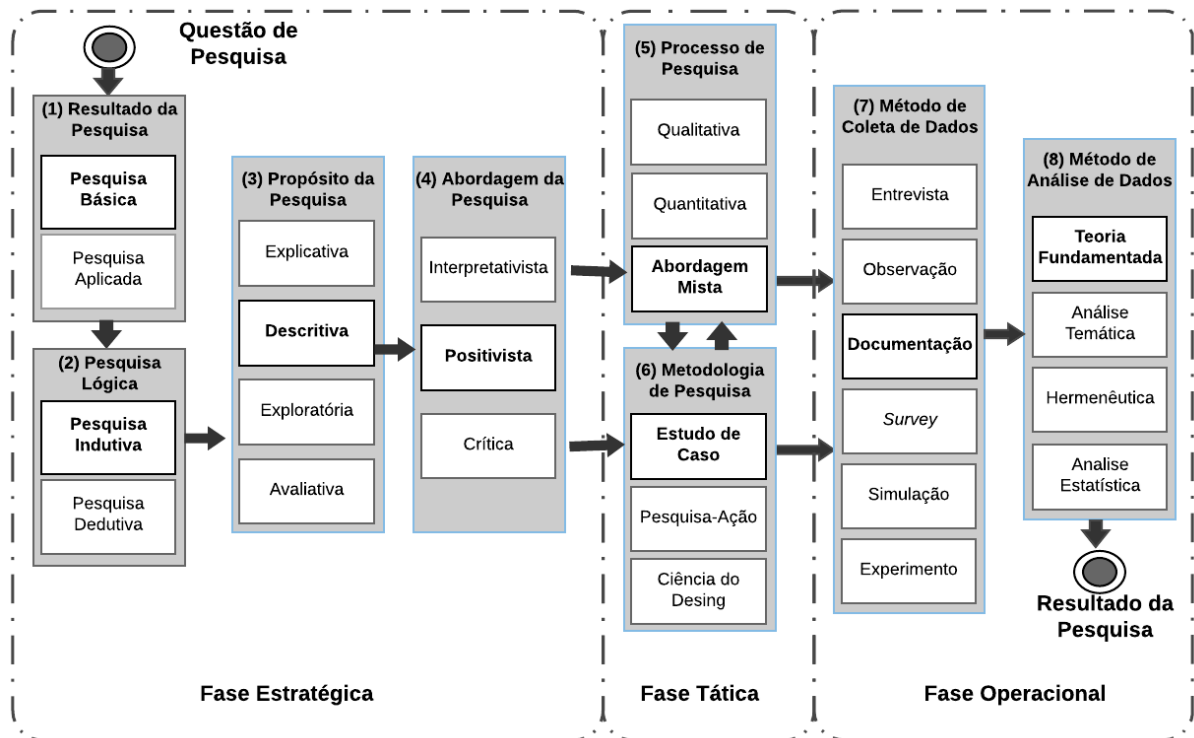
Figura 12: Estrutura de Tomada de Decisão em Pesquisa Científica. Fonte: Adaptado de Wohlin e Aurum (2015)

5.2.1.1 FASE ESTRATÉGICA

Wohlin e Aurum (2015) descrevem a fase estratégica como a fase que direciona o pesquisador para os aspectos táticos e operacionais da sua pesquisa, possibilitando a ele realizar sua pesquisa de forma sistemática. Uma estratégia para se fazer uma pesquisa eficaz requer que o pesquisador entenda o tema da pesquisa e tenha conhecimento sobre cada ponto de tomada de decisão. A estratégia de investigação envolve decidir sobre o resultado, a lógica, o propósito e a abordagem da pesquisa. Dessa forma, para o contexto desse estudo de caso, foi escolhida a pesquisa básica, indutiva, descritiva e positivista, respectivamente.

A pesquisa realizada nesse estudo é descrita como:

- **Básica**, pois segundo Wohlin e Aurum (2015) esse tipo de pesquisa é aplicada a um problema que enfatiza a compreensão do mesmo sem fornecer uma solução para ele, sendo que a principal contribuição é o conhecimento gerado a partir dessa pesquisa;
- **Indutiva** pelo fato de que o pesquisador deduz conceitos e padrões teóricos a partir da observação de dados, começando com com observações específicas para então

detectar padrões e desenvolver teorias e conclusões gerais;

- **Descritiva** pelo fato de descrever as características de um problema;
- **Positivista** pois visa que a pesquisa seja confiável, visto que ela tende a cair na categoria explicativa, onde a pesquisa é realizada em cima de dados de arquivos.

5.2.1.2 FASE TÁTICA

Seguindo com o protocolo de Wohlin e Aurum (2015), a fase tática possui dois pontos de decisão: o processo e a metodologia da pesquisa.

Existem dois tipos de processos de pesquisa: qualitativa e quantitativa. A pesquisa qualitativa tem como objetivo estudar aspectos sociais e culturais, que envolvem coleta de dados via documentação, entrevistas e observação. Já a pesquisa quantitativa enfatiza a análise de dados utilizando técnicas estatísticas e envolvem questionários, experimentos e simulações. Uma opção é a abordagem mista, resultado da combinação de fatores qualitativos e quantitativos, a qual é utilizada nesse estudo, tendo em vista que o mesmo envolve tantos dados qualitativos, quanto dados quantitativos.

Já a metodologia utilizada para que fosse possível alcançar o objetivo da pesquisa, é o estudo de caso, onde segundo o protocolo de Wohlin e Aurum (2015), esse método é uma pesquisa que pode empregar vários métodos de coleta de dados para investigar um fenômeno.

5.2.1.3 FASE OPERACIONAL

A terceira e última fase da tomada de decisão se trata das ações a serem tomadas na execução da pesquisa, e inclui o método de coleta e de análise de dados que respondem à questão de pesquisa (WOHLIN; AURUM, 2015). Como método de coleta de dados para esse estudo, foi utilizado o método de pesquisa em arquivo, ou seja, análise de documentação. Dessa forma, levando em consideração que os dados podem ser coletados de maneira qualitativa ou quantitativa, e podem fornecer evidências sobre o fenômeno estudado, para cada método de coleta podem ser usados métodos de análise diferentes. Para esse contexto foi utilizado o método da teoria fundamentada, que dá ênfase na qualidade dos métodos de analise para garantir que ela faça sentido ou que explique o fenômeno.

5.2.2 QUESTÕES DE PESQUISA

Um passo importante para a pesquisa é a definição de uma questão de pesquisa para guiar e direcionar o estudo (EASTERBROOK et al., 2008). Levando em consideração que o estudo se trata de uma pesquisa descritiva, Wohlin e Aurum (2015) descreve esse tipo de pesquisa como uma pesquisa aplicada a descrever um fenômeno ou características de um problema, onde as questões de pesquisa tendem a começar com “o que” ou “como”.

Para o contexto desse estudo foram elaboradas duas questão de pesquisa:

1. Como as falhas e/ou vulnerabilidades são identificadas nos TPS?

2. Como as falhas e/ou vulnerabilidades identificadas nos TPS são solucionadas?

Dessa forma, a QP1 busca responder se foram encontradas falhas e/ou vulnerabilidades durante a realização das edições do TPS, e quais eram essas falhas, quando encontradas. Já a QP2, busca responder de que forma as falhas encontradas pelos investigadores eram solucionadas pelo TSE. As respostas para essas perguntas estão presentes na Seção 5.3.

5.2.3 *DESIGN* DO ESTUDO DE CASO

O objetivo desse estudo é investigar a ocorrência de falhas e/ou vulnerabilidades detectadas no Sistema Eletrônico Brasileiro por técnicos e especialistas da área de segurança, durante os TPSs realizados pela Justiça Eleitoral.

Um plano de estudo de caso deve conter elementos que auxiliem a entender o que se busca e os resultados que se pretende alcançar, e para isso é necessário estabelecer alguns elementos que farão parte do estudo, como o que será estudado e qual o objetivo a ser alcançado. É importante definir uma questão de pesquisa para conduzir o estudo e os métodos de coleta de dados. Como visto anteriormente, por se tratar de um estudo descritivo, é preciso saber qual o tipo de caso de estudo será utilizado (WOHLIN et al., 2012).

O *design* do estudo de caso é único e embutido, conforme mostra a Figura 13. É considerado único porque o caso (TPS) é o evento onde são executados os planos de ataque no Sistema Eletrônico Brasileiro, e chamado embutido por tratar de múltiplas unidades de análise. Os Testes Públicos de Segurança acontecem nos anos em que antecedem as eleições, considerando que desde a criação do evento já foram realizadas quatro edições,

cada edição é considerada uma unidade de análise, dessa forma a coleta de dados e análise dos resultados deve ser realizado para cada uma das edições.
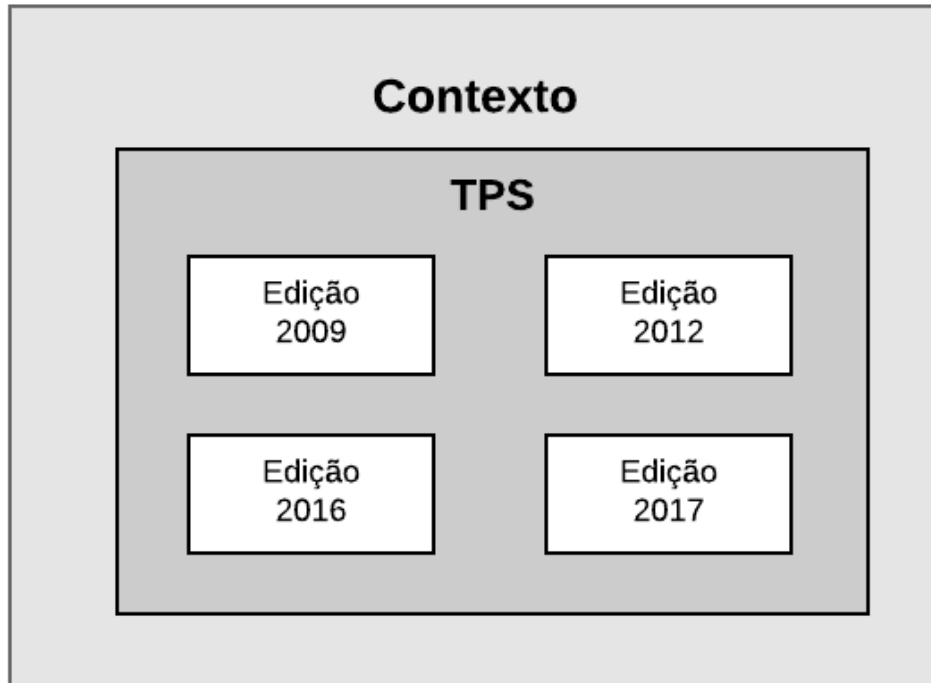
Figura 13: Tipo do projeto de estudo de caso.

Fonte: Autoria Própria

5.2.4 SELEÇÃO DE CASO

É notório a evolução pela qual o processo de votação no brasileiro passou, desde a votação em que o eleitor ditava seu voto para o escrivão, até chegarmos ao processo eletrônico utilizado atualmente. Com a informatização do voto, acabam surgindo muitas dúvidas sobre os processos eletrônicos, e dessa forma a Justiça Eleitoral criou o Teste Público de Segurança, para que quem tivesse curiosidade ou dúvidas acerca do processo atual, pudesse testar a confiabilidade do mesmo.

Sendo que até o momento foram realizados quatro edições do TPS, onde cada um possui um relatório detalhado sobre os resultados alcançados. Essa pesquisa tem como objetivo fazer um comparativo dos resultados das quatro edições, para analisar a evolução dos mesmos. Buscou-se comparar se as falhas, quando encontradas, foram solucionadas ou se voltaram a ocorrer na edição seguinte, além disso também foi analisado se esses problemas foram corrigidos antes da eleição ocorrer.

5.2.5 MÉTODOS DE COLETA E ANÁLISE

O método de coleta de dados utilizado por esse estudo foi a pesquisa em arquivo, ou documentação. A cada edição do TPS, a comissão responsável faz a documentação sobre todos os planos de ataque realizados no sistema eleitoral, bem como os resultados obtidos. Esses relatórios são publicados no site da Justiça Eleitoral.

A análise deve indicar quais foram os planos de ataque realizados no sistema eleitoral eletrônico e quais deles obtiveram ou não sucesso, além de detectar quais foram as falhas e/ou as vulnerabilidades encontradas e comprovadas pelos técnicos e especialistas que participam dos eventos. Outro fator importante é analisar se os problemas encontrados em uma edição foram solucionados, ou se foram encontrados novamente em alguma outra edição do evento.

5.3 RESULTADOS E ANÁLISE

Como mencionado anteriormente, o estudo de caso que será apresentado a seguir, segue o *desing* único e embutido, onde foram analisados os resultados de quatro edições do TPS. Para cada uma das edições, são disponibilizados pela Justiça Eleitoral os relatórios gerados a partir dos resultados obtidos pelos testes realizados. Um relatório geral de avaliação da edição em questão também é disponibilizado.

Dessa forma, a coleta dos dados foi realizada por meio de pesquisa em arquivos, os quais são arquivos públicos referentes às quatro edições do TPS. A mesma foi possível por meio do site da Justiça Eleitoral[1], onde estão disponíveis os relatórios de avaliação de todas as edições do TPS, que contemplam os planos de testes, a execução, resultados, sugestões de melhorias e a avaliação de cada teste.

O Quadro 4 mostra a visão geral das quatro edições realizadas. A primeira coluna, (I), contém a relação dos anos em que foram realizados os TPSs, seguido pela quantidade de planos de ataque realizados contra o sistema eleitoral (II) e a quantidade de planos de ataque bem-sucedidos (III) e malsucedidos (IV). Por fim, as duas últimas colunas apresentam os resultados alcançados (QP1) e as contramedidas adotadas pelo TSE (QP2), o que responde as duas questões de pesquisa definidas anteriormente na Seção 5.2.2.

A seguir, nas Subseções 5.3.1, 5.3.2, 5.3.3 e 5.3.4 são apresentados os detalhes da realização de cada uma das edições do TPS, contemplando os objetivos de cada plano

[1]http://www.justicaeleitoral.jus.br/tps/

Quadro 4: Visão geral dos resultados alcançados pelos investigadores do TPS.

I	II	III	IV	QP1	QP2
2009	9	2	7	Medição de radiação	Criptografia das teclas
2012	19	4	16	Vulnerabilidade no RDV	Melhorias no RDV
2016	11	3	8	1 - Alteração do BU 2 - Gravação de instruções de áudio	1 -Inclusão de *QRCode* com Assinatura Digital 2 - Restrição do uso de áudio e inclusão de aviso na tela da urna
2017	15	5	10	1 - Vazamento de chaves criptográficas 2 - *Bug* no sistema de assinatura digital 3 - Ausência de assinatura digital em bibliotecas	1 - Retirada das chaves do código-fonte 2 - Correção do *Bug* 3 - Diminuição do número de bibliotecas

Fonte: Autoria própria.

de ataque realizado contra o sistema, os resultados alcançados pelos investigadores e as contramedidas adotadas pelo TSE para a correção das vulnerabilidades, quando detectadas.

5.3.1 TPS 2009

Em 2009 acorreu a primeira edição do TPS, entre os dias 10 e 13 de novembro, onde 37 especialistas em informática e eletrônica, representando instituições e órgãos como *Information System Security Association*, Polícia Federal, Controladoria Geral da União (CGU), Cáritas Informática, entre outros, além de pesquisadores que também se inscreveram por conta própria participaram do evento com iniciativa de atacar o sistema eletrônico de votação brasileira para tentar encontrar alguma vulnerabilidade. O Quadro 5 apresenta a relação dos investigadores participantes dessa edição, acrescido do objetivo do seu plano de teste e seus resultados alcançados.

Com a análise realizada na documentação da Justiça Eleitoral, pode-se observar que o sistema de votação resistiu a todos os testes executados, onde nenhum conseguiu alterar o destino dos votos ou quebrar o sigilo da votação. Alguns ataques permitiram a alteração ou a inserção de arquivos, porém os mesmos não tiveram maiores consequências em virtude dos mecanismos de defesa da urna eletrônica, onde são exemplos a modificações no núcleo do sistema e ataques contra o gerador de mídias. O TSE destaca que alguns dos mecanismos de controle de segurança do sistema operacional real foram relaxados para a realização dos TPS.

Quadro 5: Visão geral dos resultados do TPS 2009.

Investigador	Integ.	Objetivo	Impacto	Resultados	Sucesso
Antônio Gil Borges de Barros	6	Analisar os mecanismos de identificação do eleitor por meio de inserção de eleitores não cadastrados na seção para permitir seu voto e possibilitar a vinculação do eleitor a seu voto falso	Desacreditação do sistema	Investigadores não obtiveram sucesso, devido ao amplo repertório de contramedidas de segurança e técnicas procedimentais adotados pelo sistema	Não
Fernando Andrade Martins Araújo	6	Avaliar as vulnerabilidades das normas e procedimentos formais que disciplinam as eleições a fim de contribuir com a transparência e padronização dos procedimentos executados durante o período eleitoral, e mitigar o risco operacional inerente a sua execução para aumentar a transparência do processo como um todo	Desacreditação do sistema	**a)** artigos insuficientes para documentar a guarda e a proteção das chaves, e falta de mais informações sobre o processo; **b)** inexistência de padronização de procedimentos para os TREs em relação ao processo de preparação das urnas e operacionalização; **c)** regras de amostragem pouco adequadas para mostrar possíveis erros; **d)** devido a complexidade e tamanho dos programas desenvolvidos, o tempo de duração do evento (5 dias), dificulta a tarefa dos representantes dos partidos conferirem os programas fonte	Sim

Continua na próxima página

Quadro 5 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Valter Monteiro Júnior	5	Introduzir código malicioso nas mídias digitais, na urna ou em qualquer servidor do sistema de votação	Desacreditação do sistema	Investigadores não obtiveram sucesso na execução do plano de teste, que se dividiu em: **a)** inserção de código malicioso em ambiente de geração de mídia: emprego de mecanismos criptográficos de segurança no sistema; **b)** comportamento dos softwares: cadeia de confiança baseada em assinatura digital estabelecida entre os aplicativos da urna que não fazem cópias de arquivos não assinados	Não
Nelson Murilo de Oliveira Rufino	1	Aplicar alteração nos arquivos de entrada de eleitores para manipular o resultado de uma eleição e permitir que os eleitores cadastrados possam votar em duas u mais seções	Desacreditação do sistema	O investigador não obteve sucesso na execução do teste devido aos mecanismos de segurança utilizados pelo Sistema Operacional da urna	Não

Continua na próxima página

Quadro 5 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Divailton Teixeira Machado	1	Executar um ataque de DoS em uma determinada urna, e quebrar o sigilo do voto por meio da análise de *logs* dos sistemas eleitorais	Quebra de sigilo de voto, sem deixar rastros	O investigador não obteve sucesso na execução do teste devido aos mecanismos de aleatoriedade do preenchimento do RDV. Já a inserção de códigos maliciosos falhou devido as camadas de segurança aplicadas ao processo	Não
Sérgio Freitas da Silva	1	Demonstrar a interceptação da radiação emitida pelo teclado da urna eletrônica através de receptores de rádio específicos. Essa radiação será rastreada, captada, digitalizada e armazenada num arquivo digital para comprovar a materialidade do fenômeno e o risco de quebra do sigilo do voto	Quebra de sigilo de voto, sem deixar rastros	O investigador teve sucesso na execução do teste, mas não comprometeu o sigilo do voto, visto que as ondas eletromagnéticas produzidas requerem uma distancia reduzida entre o aparato de captura e a urna eletrônica	Sim

Continua na próxima página

Quadro 5 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Thiago de Sá Cavalcanti	1	Subverter a geração das mídias e o programa de votação	Desacreditação do sistema	Investigador não obteve sucesso na tentativa de inserção de código malicioso, visto que a sua conjectura não pode ser totalmente testada. Destaca-se ainda, que a instalação do *root kit* só foi possível depois de desativar o antivírus	Não
Mauro César Sobrinho	3	Substituir o núcleo do sistema operacional Linux da urna, para resgatar a chave publica contida no *compact flash* e reassinar os arquivos binários presentes na urna	Desacreditação do sistema	Os investigadores conseguiram decifrar, alterar e recifrar, mas não conseguiram obter sucesso na carga do sistema, pois a urna detectou a adulteração através do sistema SAVD, que detectou a alteração no teste inicial de integridade. Os investigadores ainda tentaram adulterar o lacre, cortando, masa adulteração é perceptível	Não
Carlos Eduardo Negrão de Oliveira	1	Demonstrar a alteração do Boletim de Urna substituindo a impressora da urna eletrônica	Desacreditação do sistema	O investigador não obteve sucesso porque não foi possível reprogramar a impressora	Não

Fonte: Autoria própria.

Um dos investigadores buscou quebrar o sigilo do voto, por meio de captação da radiação eletromagnética emitida pelo teclado da urna no momento em que o eleitor está votando. Essas radiações permitem acompanhar o acionamento das teclas da urna, o que poderia levar a identificação do voto. O teste foi parcialmente bem sucedido, visto que, embora o investigador tenha conseguido captar a radiação emitida pelo teclado da urna, a distância em que o seu aparelho de rádio ficou da urna eletrônica foi de apenas cinco centímetros, o que é uma distância muito baixa, pois levando em conta que em um cenário real as urnas ficam em ambiente isolado e sob vigilância nas seções eleitorais, esse tipo de ataque é inviável. Destaca-se que uma única tecla da urna foi identificada durante o teste.

Diante deste resultado e em resposta a esse teste, as urnas fabricadas posteriormente a essa edição do TPS passaram a criptografar as teclas do terminal para que um sinal elétrico diferente seja produzido a cada vez que uma tecla seja pressionada. Assim impede qualquer tentativa de identificação de um padrão que caracteriza uma tecla específica da urna.

Além deste, investigadores da Marinha do Brasil conseguiram introduzir um arquivo na mídia de votação, porém o procedimento foi rejeitado pelo sistema da urna. Em seguida, outras duas alterações em arquivos do sistema foram imediatamente detectadas pelos módulos de segurança da urna. A alteração de um arquivo, a tentativa de geração da mídia sem o uso do gerador de mídias, e a tentativa de iniciar o sistema por meio de outro programa foram impedidas pelas barreiras de segurança do sistema eletrônico, principalmente pelas assinaturas digitais e pelo uso de mecanismos de criptografia.

Destaca-se ainda, as considerações contidas na análise dos procedimentos adotados no sistema eletrônico, que revelam que existem possibilidades de aperfeiçoamento das práticas de segurança já adotadas pelo TSE.

O primeiro TPS demostrou a robustez e segurança do sistema, resistindo a todos os ataques realizados contra o mesmo, e cumprindo o objetivo de levantar discussões para a melhoria contínua dos processos eleitorais e para determinados trechos de código do sistema de software, além de recolher sugestões para a próxima edição do evento.

5.3.2 TPS 2012

Três anos depois da primeira edição do TPS, uma nova edição ocorreu entre os dias 20 e 22 de março de 2012, onde 24 investigadores de diversas instituições foram divididos e nove grupos que executaram 19 planos de testes contra o sistema de votação

eletrônica. O Quadro 6 apresenta a relação dos investigadores participantes dessa edição, acrescido do objetivo do seu plano de teste e seus resultados alcançados.

Na edição de 2012 foi possível observar que alguns planos de ataque inscritos para o TPS não chegaram a ser executados, pois foram indeferidos pela Comissão Disciplinadora, por falta de material para a realização do mesmo, por falta de tempo hábil para a condução dos procedimentos para execução do teste ou por estar em desacordo com o escopo definido para investigação. Entre esses estavam os testes:

- Teste 1 - Grupo 2: Quebra de sigilo de voto utilizando aparelho celular;
- Teste 1 - Grupo 4: Injeção de código e violação da rotina de aleatoriedade;
- Teste 4 - Grupo 5: Quebra do Sigilo do voto eletrônico;
- Teste 1 - Investigador 3: Comprometimento da transferência dos resultados obtidos nas urnas para o servidor do TRE/TSE.

Nesse sentindo, ressalta-se ainda que alguns testes não foram realizados por não apresentarem as especificações necessárias para a confecção da interface para execução do teste, que é o caso do Teste 3 do Grupo 5, intitulado: "Tentativa de comprometimento do MSD através da interface JTAGs testes".

Dois dos testes propostos pelos investigadores, não foram executados devido a falta de tempo hábil para realização do mesmo, onde os investigadores admitiram não haver tempo suficiente para a execução, sendo eles:

- Teste 2 - Grupo 1: Tentativa não rastreável de fraude no resultado da eleição;
- Teste 4 - Grupo 4: Mapeamento do voto com o eleitor.

Por fim, o Teste 2 do Grupo 2, intitulado "Fraude no sistema de apuração utilizada no exterior" não foi realizado por ter sido deferido parcialmente pela comissão. Todos esses planos de teste não realizados foram considerados pela comissão avaliadora para fins de análise e avaliação das propostas.

Quadro 6: Visão geral dos resultados do TPS 2012.

Investigador	Integ.	Objetivo	Impacto	Resultados	Sucesso
Diego de Freitas Aranha (G1T1)	4	O teste visa quebrar o sigilo de uma votação já encerrada, ou seja, recuperar as escolhas do número máximo possível de eleitores naquela votação	Alteração do destino e quebra do sigilo do voto	O teste obteve sucesso em simulações com até 21 eleitores aleatórios, seguida por uma simulação baseada em dados reais com 580 eleitores, onde o teste recuperou 99,99% da mesma	Sim
Diego de Freitas Aranha (G1T2)	4	O teste visa alterar o resultado de uma votação já encerrada, verificando se essa hipótese é possível	Alteração do destino e quebra do sigilo do voto	O investigador não obteve sucesso na execução do teste, visto a falta de tempo para a realização do mesmo	Não
Lauro Cézar Araújo (G2T1)	2	Demonstrar vulnerabilidade de sigilo de votos diante da utilização de dispositivos eletrônicos	Quebra do sigilo do voto	O plano de teste não foi realizado, visto que foi indeferido pela comissão, visto que o se um eleitor decidir por sua livre vontade divulgar seu voto, ainda assim o eleitor esta exercendo sua liberdade. sendo assim, o sigilo do voto não esta ameaçado dessa forma	Parcial

Continua na próxima página

Quadro 6 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Lauro Cézar Araújo (G2T2)	2	Demonstrar vulnerabilidade de apuração executado no exterior ao utilizarem código verificador genérico para validar os dados do Boletim de Urna	Adulteração de resultados	A hipótese levantada se mostrou verdadeira, demonstrando que existe um ponto de melhoria possível no processo de apuração	Não
Marcelo Achar (G3T1)	3	O teste tem objetivo de tentar iniciar a urna usando memória *compact flash* com um *loadder* não assinado pelo TSE, conectar um adaptador para *ethernet* através da entrada USB, e verificar a possibilidade de clonagem da memória *flash*	Uso de código não autorizado na urna	Os investigadores não obtiveram sucesso, pois a urna não reinicializou devido a modificação do SO	Não
Marcelo Achar (G3T2)	3	O teste tem objetivo de tentar iniciar a urna usando memória *compact flash* com um *loadder* não assinado pelo TSE, conectar um adaptador para *ethernet* através da entrada USB, e verificar a possibilidade de clonagem da memória *flash*	Possibilidade de conectividade com *ethernet* com uso de adaptador	Os investigadores não obtiveram sucesso pois, além do lacre do USB violado de forma física, a urna não ofereceu nenhum tipo de IP para o dispositivo *ethernet*	Não

Continua na próxima página

Quadro 6 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Marcelo Achar (G3T3)	3	O teste tem objetivo de tentar iniciar a urna usando memória *compact flash* com um *loadder* não assinado pelo TSE, conectar um adaptador para *ethernet* através da entrada USB, e verificar a possibilidade de clonagem da memória *flash*	Clonagem da urna para manipulação de votos	Por mais que seja uma técnica viável, ela é difícil de ser aplicada devido ao grande esforço envolvido e ao numero de controles de segurança da urna e pessoas envolvidas, e os rastros poderiam ser evidentes	Não
Luís Fernando de Almeida (G4T1)	5	Simular a injeção de código a partir do compilador g++, alteração das bibliotecas para fins de mapeamento de rotina de gravação de votos	Quebra do sigilo do voto	O plano de teste foi indeferido pela comissão	Não
Luís Fernando de Almeida (G4T2)	5	Desabilitar o *flash card* para inutilizar a memória de programa gravação dos dados de votação	Inutilização do *flash card* e alteração de resultados	Teste não realizado devido à cifragem do *kernel* da urna que impossibilita o acesso ao SO	Não

Continua na próxima página

Quadro 6 – *Continuação da página anterior*

Investigador	Integ.	Objetivo	Impacto	Resultados	Sucesso
Luís Fernando de Almeida (G4T3)	5	Injeção de código malicioso através do compilador	Inutilização das urnas, cópia de dados e exclusão de dados	O teste não pode ser realizado devido a segurança existente na urna onde só foi possível acessar o código fonte, mas impossível realizar modificações para executar o teste proposto	Não
Luís Fernando de Almeida (G4T4)	5	Identificar o voto por meio do mapeamento das sementes utilizadas em cada chamada de rotina aleatória na gravação dos votos	Quebra do sigilo do voto	O teste não foi realizado por falta de tempo hábil para elaboração do mesmo	Não
Marcelo Rodrigues Souza (G5T1)	3	Modificação do *boot* da urna	Alteração do destino e quebra do sigilo do voto	Apesar do teste não ter tido ao acesso do SO, observou-se diversas possibilidades de manipulação dos parâmetros de *kernel* para *boot*. Dessa forma a alteração da inicialização abre brechas para outros ataques	Parcial

Continua na próxima página

Quadro 6 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Marcelo Rodrigues Souza (G5T2)	3	Tentativa de recuperação de dados da memória volátil	Alteração do destino e quebra do sigilo do voto	Não foi possível obter dados de alto valor visto a alta complexidade de cifragem dos mecanismos de segurança, tendo o tempo de teste como fator primordial para a impossibilidade de sucesso	Não
Marcelo Rodrigues Souza (G5T4)	3	Tentativa de comprometimento do MSD através da interface JTAG	Alteração do destino e quebra do sigilo do voto	O teste não foi realizado	Não
Marcelo Rodrigues Souza (G5T4)	3	Quebrar o sigilo do voto	Alteração do destino e quebra do sigilo do voto	Teste não realizado por indeferimento pela comissão	Indeferido
André Luis Moura dos Santos (G6T1)	4	Examinar a possibilidade de relacionar o eleitor com o voto através da análise o RDV	Quebra do sigilo do voto	O teste não obteve sucesso devido ao fato de não possuir uma fase de pre-teste, o que fez com que o grupo não conseguisse se ambientar com o sistema da urna, havendo dificuldades na execução do teste	Não

Continua na próxima página

Quadro 6 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Ricardo Antonio Pralon Santos (Individual 2)	1	Examinar os mecanismos de proteção de carga, programas da urna em fase de carga via exploração de *loader*, ataque BIOS e extensão da mesma	Alteração do destino e quebra do sigilo do voto	O investigador chegou a conclusão de que sem uma intervenção no hardware é impossível modificar os sistemas de carga e *boot* da urna	Não
Suzana Brandt Silva (Individual 3)	1	Explorar possíveis vulnerabilidades dos aplicativos de coleta de informações dos resultados durante a fase de transmissão dos mesmos diante interceptação e alteração das informações	Desacreditação do Sistema	Indeferido	Indeferido

Fonte: Autoria própria.

Devido à grande quantidade de propostas de ataques enviados ao evento para e edição de 2012, muitos deles não apresentaram nenhuma contribuição importante para o processo de aprimoramento do sistema eletrônico, onde também observou-se que os mesmos não foram devidamente concluídos, conforme apresentados nos seus respectivos planos de teste, sendo assim não avaliados pela comissão. São eles:

- Teste 1 - Grupo 3: *Boot loader* não assinado;
- Teste 2 - Grupo 3: *USB-Ethernet*;
- Teste 2 - Grupo 4: Invalidação do *FlashCard*;
- Teste 3 - Grupo 4: Proposta de execução de *ShellCode*;
- Teste 1 - Grupo 6: Teste de segurança do sistema eletrônico de votação do TSE;
- Teste 1 - Investigador 1: Extração de dados da memória RAM da urna eletrônica;
- Teste 1 - Investigador 2: Teste de exploração dos mecanismos de proteção de carga da urna.

Destaca-se a contribuição dos Grupos 2 e 6 onde, que mesmo não sendo executados, os testes apresentavam contribuições ao sistema e foram encaminhados ao TSE para avaliação. Por fim, a comissão avaliou os testes que apresentaram contribuições para para o processo. Todos, mesmo não tendo atingido o objetivo principal, apresentaram resultados relevantes.

- Teste 1 - Grupo 1: Tentativa não rastreável de quebra de sigilo do voto;
- Teste 3 - Grupo 3: Clonagem de memória *flash* de votação;
- Teste 1 - Grupo 5: Modificação do *boot* da urna;
- Teste 2 - Grupo 5: Tentativa de recuperação de dados da memória volátil do equipamento.

O Teste 1 do Grupo 1 obteve sucesso devido a um erro no RDV, onde a sequência escrita é determinística e pode ser derivada independentemente a partir dos produtos públicos de uma eleição. Ao ter a posse do RDV foi possível refazer o sequenciamento dos votos, mas não foi possível violar o sigilo visto que o grupo não conseguiu obter a

sequência de comparecimentos do eleitores, e dessa forma foi impossível relacionar os votos dos arquivo RDV com os eleitores.

Segundo o Secretário do TSE, Giusepe Dutra Janino, os resultados alcançados por esse teste é uma contribuição valiosa para o aprimoramento do processo, mas ressaltando que não existe como relacionar o voto ao eleitor, visto que para a fase de testes, a equipe teve acesso aos códigos fontes de todos os softwares executados pela urna, o que não ocorre em uma eleição real. Comentou ainda que o teste conseguiu escrever a ordem que os votos foram digitados na urna, mas seria pouco provável conseguir relacionar aos eleitores, visto que a votação ocorre por ordem de chegada, e a lista dos eleitores disponibilizada aos mesários se encontra em ordem alfabética (Tribunal Superior Eleitoral, 2012).

É importante destacar que não foi possível ter o acesso ao relatório do Investigador individual 1, o qual se tratava do teste "Extração de dados da memória RAM da urna eletrônica", porém levando em consideração o relatório geral emitido pela comissão avaliadora, o qual diz que o mesmo não apresentava nenhuma contribuição relevante para o processo, o mesmo foi desconsiderado.

5.3.3 TPS 2016

A edição seguinte do TPS foi realizada no ano de 2016, durante os dias 8, 9 e 10 de março, e contou com a participação de 13 investigadores que realizaram 11 planos de ataques contra o sistema eletrônico de votação. O Quadro 7 apresenta a relação dos investigadores participantes dessa edição, acrescido do objetivo do seu plano de teste e seus resultados alcançados.

Com a análise dos resultados obtidos pelos investigadores da terceira edição do TPS, é possível observar que houve muitos planos de ataque bem sucedidos, porém levando em consideração um cenário real, dificilmente esses resultados seriam uma ameaça ao sistema, visto que para que isso pudesse acontecer, haveria a quebra de procedimentos eleitorais, além da corrupção dos membros envolvidos.

Quadro 7: Visão geral dos resultados do TPS 2016.

Investigador	Integ.	Objetivo	Impacto	Resultados	Sucesso
Sérgio Freitas da Silva (G1T1)	1	O teste se refere ao sistema de apuração, através do Boletim de Urna, e se fundamenta na hipótese de um Boletim falso ser digitado e validado pelo sistema tornando-se legítimo	Alteração do destino dos votos	O teste foi realizado com sucesso, mas a geração de colisões de códigos verificadores de Boletim de Urna forjados, não obteve sucesso devido as características do processo eleitoral	Não
Charles Figueiredo de Barros (G2T1)	2	Captura de informações do eleitor no momento que ele é liberado pelo terminal do mesário	Adulteração do destino e quebra de sigilo do voto	O teste não foi realizado	Não
Charles Figueiredo de Barros (G2T2)	2	Verificação dos procedimentos de segurança relativos ao armazenamento de dados na memória e nas mídias	Adulteração do destino e quebra de sigilo do voto	Investigador não alcançou resultado de decifração e alteração de dados das mídias	Não
Elisabete Evaldt (G4T1)	2	Tentativa de acesso a mídia de carga da urna para inserir conteúdo de forma a permitir uma tentativa de fraude na destinação dos votos	Adulteração do destino e quebra de sigilo do voto	O testes não alcançou os resultados esperados. Várias analises foram feitas no código fonte para entender seu funcionamento e identificar pontos de vulnerabilidades, sem sucesso	Não

Continua na próxima página

Quadro 7 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Luis Fernando de Almeida (G5T1)	2	Tentativa de acoplamento de algum dispositivo que possibilite capturar o áudio disponibilizado para deficiente visual e armazenar em alguma mídia para recuperar depois e poder identificar a sequencia de votação	Adulteração do destino e quebra de sigilo do voto	O teste obteve sucesso, conseguindo transmitir o áudio do voto para os seguintes casos: urnas com áudio habilitado para todos os eleitores, votos de pessoas com deficiência visual, e votos habilitados manualmente pelo mesário	Sim
João Felipe Souza (I1T1)	1	Explorar uma falha no software que possibilita a quebra da integridade do voto, através do desligamento da urna no momento da escrita de um voto fazendo com que o eleitor seja registrado e seu voto não	Mal funcionamento da Urna	Esse teste envolve o corte de energia elétrica e da bateria da urna durante a votação do eleitor, a ideia é que no momento da confirmação do voto ocorra o desligamento da urna para que o voto não seja computado mas o eleitor seja registrado normalmente	Não
João Felipe Souza (I1T2)	1	Explorar uma falha no software que possibilita a quebra do sigilo do voto	Quebra do sigilo do voto	Atacante não obteve sucesso devido as barreiras de segurança da urna	Não

Continua na próxima página

Quadro 7 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
João Felipe Souza (I1T3)	1	Tentativa de execução de código malicioso dentro do Kit *Je Connect* para se obter acesso a VPN de transmissão de dados	Alteração dos votos no servidor	Investigado não obteve sucesso para esse teste	Não
João Felipe Souza (I1T4)	1	Tentativa de obtenção de um clone da flash de carga para *re-flashear* a urna depois da realização das eleições para simular uma eleição e redirecionar os votos	Alteração dos votos dos eleitores	O teste foi bem sucedido, mas em um cenário real, o teste implicaria na quebra de procedimentos, e na corrupção das pessoas envolvidas no processo eleitoral	Sim
João Felipe Souza (I1T5)	1	Tentativa de quebra de sigilo por meio de gravações sequenciais de registro de comparecimento e registro digital do voto	Quebra de sigilo	O teste obteve sucesso depois dos relaxamentos solicitados pelo investigador, mas em um cenário real, o teste implicaria em quebra de procedimentos além da corrupção dos envolvidos	Sim
Marcelo Muzilli (I26T1)	1	Exploração dos resultados na base de dados principal onde se concentra o resultado da votação	Adulteração do destino e quebra de sigilo do voto	O teste não foi realizado	Não

Fonte: Autoria própria.

Dentre as 11 propostas enviadas, destacam-se que 3 dos planos de ataque não foram de fato executados, por motivos de indeferimento por parte da comissão reguladora, sendo eles:

- Grupo 2: Análise da segurança do armazenamento de arquivos e valores na memória da urna e nas mídias removíveis;
- Grupo 2 : Análise das práticas de programação relacionadas ao uso de primitivas criptográficas e outros aspectos de segurança do código-fonte;
- Investigador individual: Invasão no transporte de dados no sistema de votação.

Nesse sentido, os testes realizados pelos investigadores e que não apresentaram contribuições relevantes ao processo, mesmo obtendo sucesso não foram avaliados pela comissão, sendo eles:

- Grupo 2: Ataque ao Sigilo do Voto;
- Grupo 4 : Tentativa de fraude na destinação dos votos na urna através de controle dos dispositivos de teclado e impressora;
- Investigador individual: Registrador do teclado, destruidor de votos e *Root kit JE Connect*.

Por outro lado, alguns testes obtiveram sucesso e apresentaram contribuições importantes para o aprimoramento do sistema eleitoral. Um dos investigadores conseguiu ter acesso ao BU e alterar os resultados do mesmo, utilizado-o como entrada para o Sistema de Apuração (SA) da urna, produzindo um novo BU válido com resultados fraudulentos.

Em resposta, o TSE corrigiu esse problema modificando o algoritmo do código verificador do BU, que passou a ter força de autenticador. Para adicionar uma nova camada de segurança, também foi incluído um *QRCode* com assinatura digital no BU, que permite aos interessados conferir a autenticidade e integridade do mesmo.

Além dessa vulnerabilidade, outro grupo de investigadores também teve sucesso na execução do seu plano de teste, e conseguiu fazer a gravação das instruções por áudio, utilizadas por deficientes visuais para a votação, as quais incluem as teclas pressionadas e o voto confirmado pelo eleitor. No ataque, o áudio era ativado para cada eleitor previamente cadastrado ou para todos os eleitores de uma seção previamente configurada, sem exceções. A solução apresentada pelo TSE foi restringir o uso de áudio somente para os eleitores

previamente cadastrados ou por liberação do mesário. Além disso, sempre que o áudio é ativado, é mostrada a mensagem no terminal do eleitor alertando sobre a ativação do recurso, esse recurso partiu da sugestão de um dos investigadores participantes do evento. Caso o áudio esteja ativado indevidamente, o eleitor pode solicitar ao mesário a suspensão da sua votação e a verificação de ausência de equipamentos estranhos na cabine de votação.

Além das considerações nos testes, os participantes também opinaram e fizeram sugestões quanto a realização do evento, onde as principais recomendações são que a lacração dos sistemas ocorram antes da inspeção dos códigos fonte que antecede a apresentação do plano de teste, permitir que qualquer membro da equipe possa realizar o plano de teste e elaboração de novos planos de teste adequados ao ambiente, e maior participação da comissão avaliadora durante a elaboração do TPS, além da criação de uma comissão mista permanente que seja composta por membros das 4 comissões já existentes. Outra consideração importante foi o pedido de que o TPS passe a abranger o sistema de biometria também.

5.3.4 TPS 2017

O quarto TPS foi realizado no período de 27 a 30 de novembro de 2017 e contou com 14 participantes, divididos em 4 grupos e 4 participantes individuais. O Quadro 8 apresenta a relação dos investigadores participantes dessa edição, acrescido do objetivo do seu plano de teste e seus resultados alcançados.

Os planos de teste avaliados pela comissão avaliadora que foram deferidos são:

- Investigador Marcelo dos Anjos: Teste invasão hardware/software;
- Investigador Marcelo dos Anjos: Alteração de dados da votação;
- Grupo Diego Aranha: Execução remota de código na plataforma web;
- Grupo Diego Aranha: Tentativa de violação do sigilo do voto;
- Grupo Diego Aranha: Inserção de dispositivo USB malicioso.

Quadro 8: Visão geral dos resultados do TPS 2017.

Investigador	Integ.	Objetivo	Impacto	Resultados	Sucesso
Cassio Goldschmidt	1	Encontrar erros e vulnerabilidades no software responsável pela carga das urnas que possibilitem a inserção de código dentro desse sistema, a fim de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados e dos sistemas responsáveis pela votação eletrônica	Desacreditação do Sistema	O investigador não conseguiu cumprir o objetivo proposto neste plano de teste. No entanto, apontou alguns itens de não conformidade com boas práticas do mercado, que, no entender da comissão avaliadora, devem ser considerados pela equipe técnica do TSE na revisão dos processos adotados	Não
José Carlos Gama Quirino	1	Ataques genéricos à urna eletrônica, na tentativa de comprometer a integridade e o anonimato do voto	Quebra de sigilo do voto	O investigador não conseguiu cumprir o objetivo nos testes propostos, e não houve nenhuma contribuição	Não
Marcelo dos Anjos	1	Atacar o hardware de segurança da urna eletrônica com a intenção de extrair desse dispositivo informações confidenciais do sistema de votação eletrônico	Quebra de sigilo do voto	O teste não foi realizado	Não

Continua na próxima página

Quadro 8 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Marcelo dos Anjos	1	Alterar dados de votação da urna eletrônica por meio de ataque ao sistema responsável pela transmissão dos arquivos de urna	Quebra de sigilo do voto	O teste não foi realizado	Não
Rodrigo Cardoso Silva	1	Invadir o sistema responsável pela recepção dos arquivos de urna eletrônica a partir de ataques ao sistema de transmissão desses mesmos arquivos	Desacreditação do sistema	O investigador não conseguiu cumprir o objetivo nestes dois planos de testes propostos e não houve nenhuma contribuição	Não
Rodrigo Cardoso Silva	1	Explorar vulnerabilidades do sistema operacional que roda na urna eletrônica, podendo por meio dele alterar ou prejudicar os sistemas e os dados contidos na urna	Alteração de votos e quebra de sigilo do voto	O teste não foi realizado	Não

Continua na próxima página

Quadro 8 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Diego de Freitas Aranha	6	Capturar a chave secreta da urna eletrônica, por meio de ataques ao cartão de memória utilizado para fazer carga nas urnas	-	Os resultados obtidos da execução do plano de teste não violaram a destinação e/ou anonimato dos votos. A obtenção da chave criptográfica do cartão de memória que realiza a carga do sistema da urna devido ao acesso à chave que estava no código-fonte de testes e também em porção desprotegida do sistema de arquivos do cartão. A decrepitação do cartão de memória de carga permite a inspeção de partes críticas do software e vazamento de outras chaves criptográficas sensíveis	Sim
Diego de Freitas Aranha	6	Atacar os equipamentos e sistemas responsáveis pela recepção e transmissão dos arquivos de urna eletrônica	-	O teste não foi realizado	Não

Continua na próxima página

Quadro 8 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Diego de Freitas Aranha	6	Encontrar vulnerabilidades no algoritmo de aleatoriedade do Registro Digital do Voto (RDV), buscando fragilizar o sigilo do voto	-	O teste não foi realizado	Não
Diego de Freitas Aranha	6	Atacar a urna eletrônica executando sistema malicioso, por meio das entradas USB do equipamento	-	O teste não foi realizado	Não
Diego de Freitas Aranha	6	Execução de código estranho de impressão na urna eletrônica	-	Aponta a possibilidade de alteração de parâmetros e de funcionalidades da biblioteca, onde foi alterado o formato de mensagem de *log* e inserido um texto anômalo na inicialização do sistema. Os resultados obtidos da execução do plano de testes não violaram a destinação e/ou anonimato dos votos	Sim

Continua na próxima página

Quadro 8 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Diego de Freitas Aranha	6	Violação do sigilo do voto individual sensível	Quebra de sigilo do voto	Foi realizado um ataque a biblioteca utilizada para cifrar o arquivo RDV, após verificação que esta não estava assinada. Existe possibilidade de decifração do arquivo RDV possibilitando uma possível quebra do sigilo do voto se for possível acumular sucessivas versões do arquivo, antes e depois de cada voto	Sim
Diego de Freitas Aranha	6	Violação da integridade do software de votação	Quebra de sigilo do voto	Ataque a biblioteca utilizada no sistema eletrônico de votação após verificação que esta não estava assinada. Existe a possibilidade de interferência no funcionamento do sistema eletrônico de votação através da alteração de uma mensagem constante na tela da urna	Sim

Continua na próxima página

Quadro 8 – *Continuação da página anterior*

Investigador	**Integ.**	**Objetivo**	**Impacto**	**Resultados**	**Sucesso**
Luis Antonio Brasil Kowada	4	Avaliar se os procedimentos de gerenciamento da chave secreta da urna eletrônica garantem a confidencialidade e a autenticidade necessárias	Quebra de Sigilo do voto	O investigador não conseguiu cumprir o objetivo nos testes propostos, e não houve nenhuma contribuição	Não
Ivo de Carvalho Peixinho	3	Executar o software da urna eletrônica em um computador e, a partir daí, tentar extrair a chave secreta da urna eletrônica	-	Ataque ao sistema de inicialização da urna e obtenção da chave criptográfica utilizada pelo módulo do *kernel*. possibilidade teórica de construção de programa que assine os produtos de uma urna (modelo anterior a 2009, sem MDS7), que provavelmente seria aceito pelo totalizador	Sim

Fonte: Autoria própria.

Já os testes realizados, em que os investigadores não conseguiram cumprir com o objetivo do teste e não apresentaram nenhuma contribuição para o aprimoramento do processo, foram:

- Investigador Rodrigo Cardoso Silva: Programa Transportador de Arquivos: teste *Doodle* e *Uenux* e softwares básicos Metamorfose (Kafka);
- Investigador José Carlos Gama Quirino: Ataque aos sistemas dos hardwares e softwares da urna eletrônica;
- Grupo Luís Antônio Brasil Kowada: Análise do uso dos procedimentos criptográficos.

Em contra partida, vários testes foram realizados com sucesso, apresentando diversas contribuições para o processo.

O Investigador Cássio Goldschmidt, que aplicou a revisão de código e teste dinâmico de geração das mídias para a preparação da urna eletrônica (GEDAI-UE), não conseguiu cumprir o objetivo proposto, mas apontou alguns itens de não conformidade com as boas práticas do mercado, que, no entender da comissão avaliadora, devem ser considerados pela equipe técnica do TSE na revisão dos processos adotados.

O Grupo do investigador Diego Aranha realizou diversos testes de ataque contra o sistema, entre eles, ataques contra a criptografia do sistema de arquivos do cartão de memória, e ataque a biblioteca de registro de histórico de atividades contida no sistema eletrônico de votação após verificação que esta não estava assinada. Os impactos mostram a possibilidade de alteração de parâmetros e de funcionalidades da biblioteca, mas os resultados obtidos da execução do plano de testes não violaram a destinação ou anonimato dos votos.

O Grupo ainda realizou o teste de violação de sigilo de voto individual sensível, por meio do ataque a biblioteca utilizada para cifrar o arquivo RDV, e teste de violação da integridade do software de votação realizando o ataque contra a biblioteca utilizada no sistema eletrônico de votação após a verificação que estas não estavam assinadas. Os impactos da possibilidade de decifração do arquivo RDV podem causar uma possível quebra do sigilo do voto e gerar interferência no funcionamento do sistema eletrônico de votação por meio da alteração de uma mensagem constante na tela da urna.

Por último, o grupo de Peixinho executou o software da urna eletrônica em um computador para tentar extrair a chave secreta da urna eletrônica. O ataque ao sistema de inicialização da urna e obtenção da chave criptográfica utilizada pelo módulo do *kernel*

possibilita a teoria da construção de programa que assine os produtos de uma urna que provavelmente seria aceito pelo totalizador.

Resumidamente, o vazamento da chave de criptografia das mídias da urna no ambiente de inspeção de código-fonte, *bug* no mecanismo de verificação de assinatura digital de bibliotecas e ausência de assinatura digital complementar em duas bibliotecas do sistema, foram as principais falhas encontradas no TPS de 2017.

Nesse sentido, o TSE trabalhou para a correção dessas vulnerabilidades, onde o *bug* no mecanismo de assinatura foi corrigido e a quantidade de bibliotecas foi reduzida. Os processos de testes de software também foram aprimorados incluindo assinatura devidamente validada em todos executáveis, e todas as chaves foram retiradas do código-fonte do software da urna.

Um outro ponto observado foi a capacidade de inicialização do sistema operacional da urna em ambiente virtual objetivando a realização de uma possível engenharia reversa afim da obtenção das chaves criptográficas. Em resposta, o TSE reforçou a criptografia do sistema operacional de uma forma que somente a urna seja capaz de decifrar e iniciar o sistema.

5.4 AMEAÇAS À VALIDADE DA PESQUISA

Uma questão muito importante para os resultados de experimentos, é a validade dos seus resultados. Para Wohlin et al. (2012) primeiramente deve-se validar os resultados para a população onde a amostra é coletada, e depois generaliza-los à uma população mais ampla. Dessa forma, existem diferentes tipos de validar um experimento, entre elas a validade de conclusão, construção, interna e externa.

1. Conclusão: é referente à relação estatisticamente significativa entre o tratamento e os resultados Wohlin et al. (2012). Dessa forma é importante levar em consideração que o estudo de caso foi realizado por meio de consulta em arquivo, existindo a possibilidade da existência de documentos importantes para o estudo, podendo conter informações relevantes ao contexto estudado que não são disponibilizados pelas entidades responsáveis, visto a confidencialidade aplicada aos mesmos, visto que podem conter informações relevantes ao contexto do estudo.

2. Interna: Esse tipo de validade, segundo Wohlin et al. (2012) refere-se à relação causal entre o tratamento e os resultados. Sendo assim, a ameaça a validade interna

é observada diante à dificuldade da leitura de alguns documentos relacionados a pesquisa. Esses documentos são arquivos de baixa qualidade por se tratar de documentos que foram impressos, preenchidos e escaneados, dificultando a leitura e extração de dados tendo em vista a imagem escurecida ou apagada..

3. Construção: diz respeito à relação entre teoria e aplicação Wohlin et al. (2012). A identificação dessa ameaça esta relacionada ao fato de que não foi possível ter acesso a alguns relatórios individuais de investigadores, relatório esse que possuia o detalhamento do plano de ataque a ser realizado contra o sistema eleitoral brasileiro.

4. Externa: A validade Externa refere-se à generalização de resultados num campo externo ao estudo Wohlin et al. (2012), considera-se como ameaça a esse tipo de validade a realização de testes no sistema eleitoral que não são públicos, e sim realizados pela própria Justiça Eleitoral, os quais podem resultar em alguma vulnerabilidade e falha que já são corrigidas sem que sejam divulgadas para o público.

5.5 CONSIDERAÇÕES FINAIS

O presente capítulo apresentou o estudo de caso realizado para essa pesquisa. O mesmo foi feito sob a documentação gerada a partir da realização dos Testes Púbicos de Segurança, evento promovido pela Justiça Eleitoral com o intuito de aprimorar o sistema eletrônico brasileiro.

Levando em consideração os ataques realizados contra o sistema eletrônico, muitas contribuições foram apresentadas ao TSE para que o sistema fosse cada vez mais aprimorado. Muitos ataques foram executados com sucesso, apontando brechas ou vulnerabilidades no sistema que puderam ser corrigidos pelo TSE, em contra partida, os ataques mal sucedidos puderam mostrar que a urna possui muitos mecanismos de defesa que são eficazes para proteger o eleitor de ter seu voto revelado e garantir a integridade da eleição.

O TPS que mais detectou problemas foi a edição de 2017, onde vulnerabilidades como vazamento da chaves criptográficas, *bug* no mecanismo de verificação de assinatura digital de bibliotecas e ausência de assinatura digital complementar em bibliotecas do sistema foram detectadas. Essas vulnerabilidades se não detectadas, poderiam comprometer a segurança do sistema, dessa forma, assim que encontradas foram corrigidas pela equipe do TSE. Ressalta-se a importância da realização do TPS para o TSE, visto o grande número de contribuições geradas a partir dos ataques executados contra o sistema, que contribuem de forma significativa para o constante aprimoramento do mesmo.

6 SISTEMA ELEITORAL BRASILEIRO: UMA ANÁLISE COMPARATIVA COM SISTEMAS DE VOTAÇÃO ELETRÔNICA SUPERVISIONADA AO REDOR DO MUNDO

Além do Brasil, diversos outros países do mundo fazem uso do voto informatizado em suas eleições (Figura 14). Segundo dados do *International Institute for Democracy and Electoral Assistance* (IDEA), sistemas de votação e captação de votos eletrônico são utilizados em 35 países. Entre esses estão a Suíça, Canadá, Austrália e alguns estados dos Estados Unidos. Além disso, quase toda a América Latina, alguns países da Europa, Federação Russa, Oceania Japão, China, Coréia do Sul entre outros.

O IDEA é uma organização intragovernamental que apoia a democracia sustentável em todo o mundo, e já possui diversos países membros, como Austrália, Canadá, Alemanha, Índia, Portugal, Uruguai, entre outros (International Institute for Democracy and Electoral Assistance, 2015). Fundado em fevereiro de 1995 em Estocolmo - Suécia, com o objetivo de estabelecer e manter a democracia ao redor do mundo, mais de 20 anos depois o seu trabalho vem se tornando cada vez mais forte devido ao grande número de ataques contra a democracia e debates sobre como ela é regida (Confederação Nacional das Instituições Financeiras, 2016).

O Brasil é membro do IDEA desde o ano de 2016 quando o TSE e o Ministério de Relações Exteriores estabeleceram o termo de cooperação para oficializar a adesão do país ao Instituto. Essa decisão não foi fortemente apoiada pelos três poderes do Estado (Executivo, Legislativo e Judiciário), visto que levou cerca de um ano e dois meses para que o processo de adesão fosse concluído. Essa adesão foi classificada como "altamente significativa" pelo diretor do IDEA para a América Latina, destacando que o Brasil vem desempenhando um papel de líder regional e ampliando a sua presença no meio internacional. Segundo ele, o papel que o TSE vem desempenhando no campo eleitoral, com o voto eletrônico e cadastramento biométrico, constitui um modelo que é levado em consideração não somente a nível da América Latina, como no mundo todo (Tribunal Superior Eleitoral, 2016b).
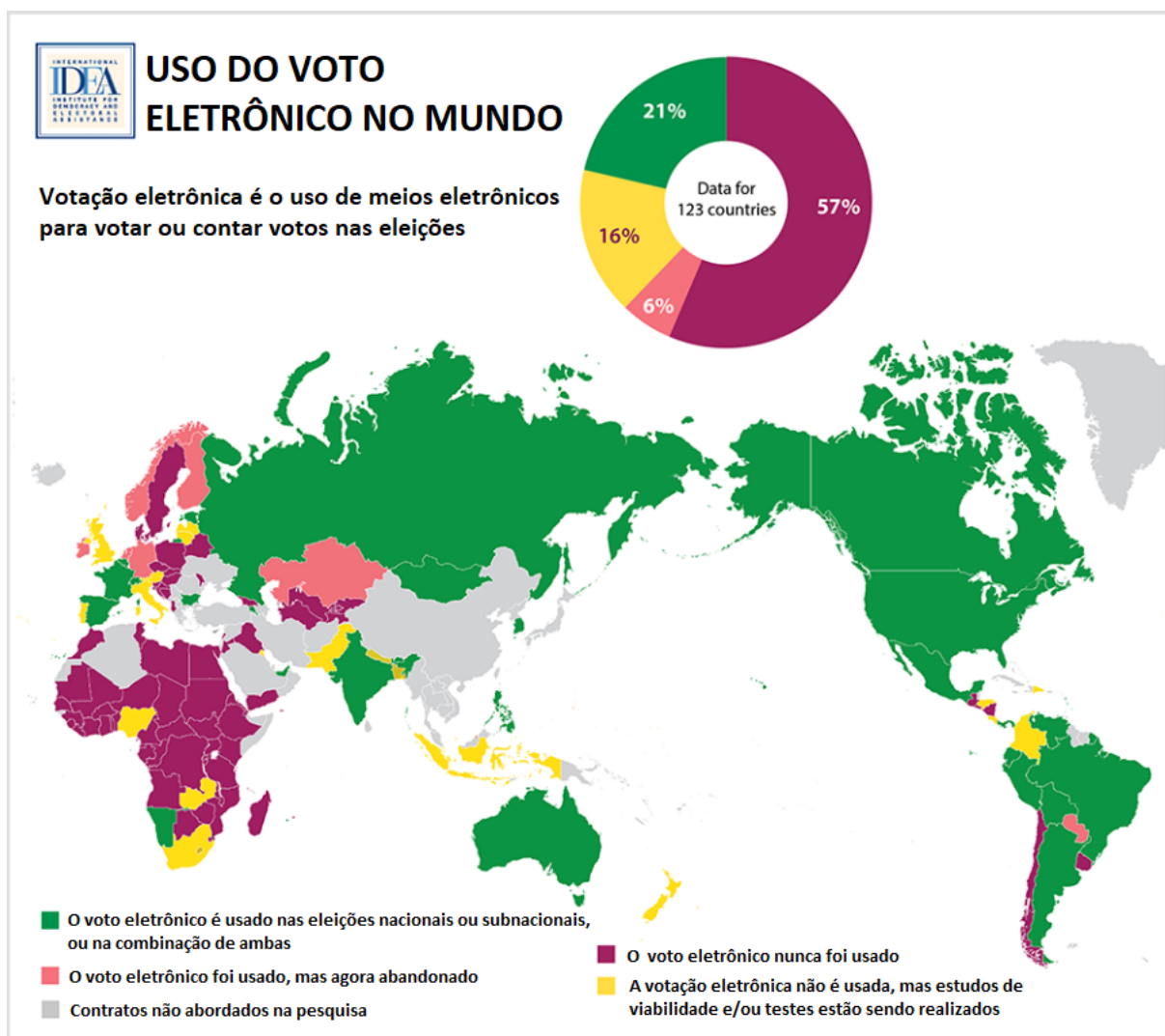
Figura 14: Relação dos países que utilizam meios eletrônicos nas eleições.

Fonte: Adaptado de International Institute for Democracy and Electoral Assistance (2015).

Devido ao avanço tecnológico, cada vez aparecem mais sistemas eletrônicos destinados a informatizar algum tipo de processo com o objetivo de automatizar e facilitar os procedimentos relacionados e eles, como por exemplo sistema bancários, onde atualmente já existem banco totalmente digitais, sistemas utilizados em universidades que visam facilitar o envio e recebimento de documentos sem que esse seja feito por transporte físico, sistemas de ouvidorias, entre outros. Todos esses sistemas possuem propriedades que garantem ao usuário que as principais propriedades de segurança, como a autenticidade e integridade e a anonimidade sejam atendidas. Assim como vários sistemas se tornaram digitais ao longo dos anos, o sistema de votação também se tornou informatizado, como já visto anteriormente, esse processo começou a ganhar forma no ano de 1996, e atualmente

o sistema utilizado é o de votação supervisionada, que Zissis e Lekkas (2011) define como o tipo de votação que ocorre diante de autoridades eleitorais, utilizando-se de urnas eletrônicas físicas para a coleta dos votos.

Tendo em vista que sistemas eletrônicos estão suscetíveis a tentativas de invasão por meio de ataques, os sistemas eleitorais também estão sujeitos a essas ameaças. Sendo assim, a Justiça Eleitoral criou os Testes Públicos de Segurança, a fim de testar e manter o aprimoramento constante do sistema eleitoral brasileiro. Comparado a outros sistemas de eleições supervisionadas implementados por outros países, é possível observar certas semelhanças e diferença entre os mesmos, das quais serão abordadas na Seção seguinte.

O presente Capítulo, visa efetuar uma análise comparativa entre o sistema de votação eletrônica utilizado no Brasil com os sistemas de votação supervisionada utilizados ao redor do mundo, destacando as características mais relevantes de cada sistema. A Seção 6.1 apresenta quais foram as vulnerabilidades detectadas no sistema eleitoral brasileiro, tendo como base os resultados alcançados com o Estudo de Caso realizado no Capítulo 5. A seção seguinte, 6.2, apresenta as características dos sistemas de votação supervisionada retornados com o MS realizado no Capítulo 4. Por fim, uma comparação do sistema brasileiro com os demais sistemas utilizados em outros países, é feita no Seção 6.3 e as considerações finais do Capítulo são apresentadas na Seção 6.4.

6.1 VULNERABILIDADES NO SISTEMA ELEITORAL BRASILEIRO

Durante a primeira edição do TPS no ano de 2009, investigadores conseguiram detectar vulnerabilidades no processo eleitoral, não só na urna eletrônica, mas também na condução do processo. Um dos grupos, por meio da análise dos processos aplicados à condução das eleições, detectou inconformidades nas documentações, as quais não influenciavam diretamente nos resultados obtidos através da urna, apenas nos procedimentos realizados para a condução das eleições. Contudo, outro grupo conseguiu detectar uma vulnerabilidade de quebra de sigilo do voto que poderia comprometer a anonimidade do voto do eleitor. Se trata da captação de radiação eletromagnética da urna permitindo escutar o acionamento das teclas.

Embora o ataque tenha sido bem sucedido, foi comprovado que esse tipo de ataque era impossível ser realizado em um ambiente real, visto a pequena distância em que o atacante precisaria estar da urna para que conseguisse captar a radiação, e levando em conta que o ambiente de votação é supervisionado, dessa forma o atacante não conseguiria

realizar o ataque. Mesmo assim, o TSE desenvolveu medidas que resolvessem esse problema, por meio da criptografia das teclas fazendo com que cada uma emitisse um sinal diferente cada vez que uma tecla fosse pressionada, para que dessa forma fosse impossível estabelecer um padrão para identificação dos números digitados pelo eleitor.

Na edição seguinte, uma vulnerabilidade no RDV fez com que os investigadores obtivessem sucesso no ataque a urna. Nessa ocasião, o grupo conseguiu refazer o sequenciamento do registro dos votos, o que poderia novamente comprometer a anonimidade do eleitor se não fosse o fato de que não foi possível obter a lista de comparecimento dos eleitores na seção eleitoral, sendo impossível relacionar um voto a um eleitor específico. Além disso, a lista de comparecimento dos eleitores que fica em mãos dos mesários se encontra em ordem alfabética, e a assinatura dos eleitores que já votaram é feita por ordem de chegada, sendo assim, não há a possibilidade de vincular a sequência dos votos com a lista de comparecimento dos eleitores.

Já em 2016, muitos dos planos de ataque dos investigadores foram realizados com sucesso, obtendo bons resultados. Porém, se tratando de um cenário real, são ataques improváveis devido ao fato da supervisão das seções eleitorais. Em contrapartida um dos grupos de investigadores conseguiu acesso ao BU e conseguiu alterar os resultados gravados no mesmo, o que mostra que essa é uma vulnerabilidade capaz de comprometer a integridade do sistema visto a alteração sem autorização dos resultados da eleição. A correção aplicada a essa vulnerabilidade deu origem ao *QRCode* com assinatura digital no BU além da modificação no algoritmo do mesmo que passou a ter força de autenticador.

Ainda na edição de 2016, o TPS identificou outra falha no sistema que conseguia fazer a gravação das instruções por áudio que o sistema oferece aos deficientes visuais das seções. Nesse caso, o áudio era ativado para todos os eleitores comprometendo a anonimidade do voto. Seguindo sugestões dos investigadores responsáveis por esse ataque, o TSE restringiu o uso do áudio apenas para eleitores previamente cadastrados ou por liberação do mesário. Além disso, a urna passou a apresentar uma mensagem na tela toda vez que o áudio é ativado, para que dessa forma um eleitor que não tenha solicitado o áudio possa identificar a adulteração.

Na última edição do evento, vários problemas relacionados ao sistema eletrônico de votação foram identificados, como o vazamento de chave criptográfica do sistema da urna eletrônica, *bug* no sistema de assinatura digital e ausência de assinatura digital em bibliotecas do código. Essas vulnerabilidades combinadas poderiam comprometer a autenticidade e a integridade do sistema. O TSE trabalhou para a correção dessas

vulnerabilidades corrigindo o *bug* das assinaturas e reduzindo o número de bibliotecas. Para o problema das chaves criptográficas, a solução foi retirá-las no código-fonte. Outra medida de segurança aplicada ao sistema depois do TPS de 2017, foi o reforço da criptografia do sistema operacional a fim de que as chaves criptográficas fossem decifradas apenas pela urna para então iniciar o sistema, essa medida foi tomada, para evitar uma possível engenharia reversa no sistema inicializando-o em ambiente virtual.

6.2 CARACTERÍSTICAS DOS SISTEMAS ELEITORAIS DE OUTROS PAÍSES

Os países que utilizam meios eletrônicos para as eleições, presentes na Figura 14, utilizam diferentes tipos de coletores de voto. Levando em consideração os estudo retornados pelo MS presente no Capítulo 4, alguns dos estudos se referem diretamente a sistemas eleitorais que seguem os mesmos princípios do que é utilizado no Brasil, ou seja, votação supervisionada. Diante disso, pelos resultados obtidos foi possível observar que os sistemas estrangeiros apresentam algumas falhas, onde os autores apresentam propostas e abordagens para alguma solução que possa mitigar essas ameaças.

O estudo de Gurubasavanna et al. (2018) aborda o sistema eleitoral utilizado na Índia, um país com uma das maiores democracias do mundo, o qual também substituiu o esquema de voto em papel por máquinas eletrônicas. No estudo os autores abordam a possibilidade do eleitor votar em qualquer seção eleitoral mesmo que ele seja pertencente a outra seção. Os autores explicam que o processo pode ser mais seguro ao envolver a autenticação baseada em impressão digital juntamente com os recursos de reconhecimento de face e íris. Eles utilizam *raspberry pi* para a construção do protótipo e discutem como pode ser utilizado.

A Índia adotou o sistema eletrônico em 1982, e desde 2003 todos os estados indianos votam com as EVMs (*Electronic Voting Machines*), uma máquina de votar que mistura de papel com meios digitais. Nessa urna, o eleitor tem a sua disposição uma cédula de papel fixo no lado esquerdo da máquina com os nomes dos candidatos. Para votar, é preciso pressionar um botão no lado direito, o qual corresponde ao nome do candidato. Também tem a possibilidade de anular a voto, por meio de um botão que funciona do mesmo jeito, porém esses votos nulos são depositados em urnas diferentes. Cada voto é transferido por fio a uma unidade de controle que fica na mão do mesário, que é responsável por autenticar a liberar o voto de cada eleitor, que recebe um comprovante de voto de papel (Olhar Digital, 2018).

Antes de votar o eleitor precisa ser autenticado, semelhantemente ao que acontece no processo eleitoral brasileiro, o nome do eleitor é conferido na lista de votantes da seção, e seu dedo indicador da mão esquerda é examinado para ver se existe alguma marca com tinta indelével[1], caso não tenha, a marca é feita na hora e então ele é liberado para votar.

Outro estudo sobre eleições supervisionadas é o de Babenko e Pisarev (2018), o qual foi publicado na Rússia e realiza uma análise de um protocolo de criptografia usado no sistema de votação eletrônica com base em assinaturas cegas (*Blind signature*[2]). Para análise da segurança desse protocolo os autores utilizam a ferramenta Avispa[3], cujo objetivo era testar a criptografia do protocolo quanto a resistência a ataques de autenticação. Nesse sentido foi realizado o ataque MITM (*Man-in-the-Middle*), ou "ataque do homem no meio", onde a análise preliminar realizada pelos autores mostra que os dados transmitidos pelo protocolo estão seguros visto a criptografia aplicada aos dados.

Pereira e Wallach (2017) descrevem como os ataques de choque podem enfraquecer as garantias de segurança do *STAR-Vote*, um sistema criptográfico de ponta a ponta utilizado em algumas regiões dos Estados Unidos da América que produz cédulas em papel de texto simples e registros eletrônicos criptografados, e possui uma variedade de mecanismos de segurança. Por fim, os autores concluem que esse sistema é capaz de detectar fraudes e fornecer aos funcionários eleitorais evidências redundantes do que aconteceu durante a eleição.

Um sistema de votação eletrônica criptografada é proposto por AboSamra et al. (2017), com o objetivo de substituir os métodos de votação convencionais utilizados no Oriente Médio e África. Esse sistema é baseado no conceito do *Prêt à Voter*, um esquema de votação eletrônica em cédulas. A proposta é simples e, segundo os autores, também é seguro, prático e auditável e a avaliação de segurança é realizada com base nas propriedades críticas e desejáveis do voto eletrônico. Depois da análise dos resultados, os autores concluem que esse esquema de votação fornece aos eleitores uma experiência de votação muito semelhante aos já utilizados, demonstrando-se flexível e adaptável e podendo apoiar vários métodos de votação, sendo um forte candidato de sistema a ser implantado. Dessa forma, para que sejam substituídos os métodos de votação convencionais nos países em desenvolvimento a proposta desse estudo tem o potencial para ser implantada como um

[1]Tinta especial utilizada para as eleições da Índia. Fabricada por apenas dois químicos que conhecem a fórmula secreta, sobre um forte esquema de segurança a tinta é feita para durar por semanas sem sair da pele (Uol - Folha de São Paulo, 2018).

[2]Tipo de criptografia baseada em assinatura digital em que o conteúdo de uma mensagem é disfarçado antes de ser assinado.

[3]Ferramenta utilizada para auxiliar o projeto e a verificação automática de protocolos.

sistema de votação eletrônica confiável. Os autores ainda pensam em estender a pesquisa para que o sistema possa acomodar métodos de votação mais complexos.

Babenko, Pisarev e Makarevich (2017) levantam a questão da criação de um sistema de votação aberto e implementado usando algoritmos criptográficos padronizados da Federação Russa, propondo um modelo baseado em intermediários cegos, que usa algoritmos de criptografia com cifra simétrica e função de *hash*. O modelo foi desenvolvido para que a intervenção humana que poderia influenciar os resultados fosse eliminada, além de impedir que qualquer pessoa pudesse votar. Os autores concluem que o modelo proposto fornece mecanismos capazes de conduzir a votação corretamente, visto que o mesmo é capaz de transmitir os dados confidenciais com segurança e fazer a distribuição de chaves secretas, autenticação mútua das partes e verificação dos dados transmitidos quanto à integridade e tempo de controle.

O estudo de Lavanya (2011) analisa o software e o hardware de uma máquina de votar a fim de verificar a segurança da mesma, expondo-a a execução de código malicioso para o roubo de votos de um candidato para outro, e acesso físico a máquina para inserção de cartões de memória. Depois da realização de vários ataques, o autor mostra que a máquina se mostrou vulnerável a vários deles, colocando em dúvida a precisão e a credibilidade da contagens de votos. Apesar de o estudo ter sido realizado na Índia, o autor não especificou qual foi o tipo de máquina de votar utilizada para os testes, e nem se a mesma é utilizada no país.

6.3 O SISTEMA ELEITORAL BRASILEIRO COMPARADO AOS SISTEMAS UTILIZADOS EM OUTROS PAÍSES DO MUNDO

Como já visto anteriormente os sistemas de votação eletrônico podem ser classificados em supervisionados: aqueles onde a eleição é realizada perante membros da justiça eleitoral e em lugares e datas específicos; e remotos, que a votação é de exclusiva responsabilidade do eleitor, podendo ser realizada via Internet. Levando em consideração que o sistema utilizado no Brasil, trata-se de um sistema de votação supervisionado, buscou-se fazer uma comparação entre os demais sistemas supervisionados do mundo, com o sistema brasileiro.

Como base para essa comparação, foram levados em consideração os resultados obtidos com o MS (Capítulo 4) e os resultados obtidos pelo estudo de caso presente no Capítulo 5. Tal comparação foi realizada com a finalidade de elencar pontos positivos e negativos do sistema brasileiro, quando comparado ao sistema desses países.

O Quadro 9 apresenta a visão geral da comparação entre os sistemas de votação eletrônica supervisionada do mundo, onde na primeira coluna (País/Região) é especificado de qual país ou região se trata o sistema de votação em questão. A segunda coluna (Propriedade), diz respeito à qual propriedade do sistema de votação está sendo abordado. A terceira coluna (Sistema do País), tem como objetivo elencar as características do sistema utilizado pelo país que está sendo comparado com o Brasil. Da mesma forma, a quarta coluna (Sistema Brasileiro) apresenta as características do sistema brasileiro em comparação com o sistema do outro país.

Quadro 9: Diferenças entre os sistemas eletrônicos de votação supervisionada.

País/Região	Propriedade	Sistema do País	Sistema Brasileiro
Índia	Autenticação	Autentica o eleitor com marcação utilizando tinta indelével	Autenticação biométrica
Índia	Credibilidade	Testes realizados em máquina de votar põe em dúvida a credibilidade do sistema	Sistema brasileiro se mostrou resistente à vários tipos de ataques
Rússia	Criptografia	Protocolo baseado em assinaturas cegas resiste a ataques de autenticação	Algorítimos de cifragem simétrica e assimétrica garantem a privacidade do eleitor
EUA	Detecção de Fraudes	*STAR-Vote* é capaz de detectar fraudes e fornecer evidências do que aconteceu durante a eleição	Possui uma grande variedade de mecanismos de segurança que são capazes de detectar fraudes
Oriente Médio e África	Protocolo	Proposta de sistema flexível e adaptável baseado no *Pret-à-Voter*	Semelhança na proposta de eliminação da intervenção humana

Fonte: Autoria própria.

Em seguida, é apresentado detalhadamente a comparação entre os sistemas de votação supervisionados utilizados no mundo, comparados com o sistema brasileiro.

Sendo assim, é possível observar que o sistema de votação utilizado na Índia, apresentado por Gurubasavanna et al. (2018) apresenta diferenças significativas quanto ao processo de autenticação do eleitor, visto que no Brasil o processo de autenticação atualmente vem sendo feito por meio de biometria, e por hora ainda não foram realizados testes públicos para tentativas de fraude da autenticação, porém já é algo sugerido pelos investigadores das edições passadas ao TSE implantar na próxima edição do evento.

Já a comparação com o sistema abordado no estudo de Babenko e Pisarev (2018),

o sistema brasileiro utiliza algoritmos proprietários de cifragem simétrica e assimétrica, que é de conhecimento exclusivo do TSE. Nesse algoritmo o BU é criptografado de forma segmentada, assinado digitalmente e transmitido. Outro mecanismo de segurança aplicado ao sistema é a descriptografia, processo pelo qual são recuperados os dados previamente criptografados (Tribunal Superior Eleitoral, 2019a).

Segundo o TSE, o processo ocorre da seguinte forma no recebimento do BU:

1. Validação da compatibilidade da chave pública de assinatura digital do BU com a chave privada do Totalizador;
2. Descriptografia do BU de forma segmentada;
3. Leitura do BU descriptografado;
4. Armazenamento do boletim de urna criptografado e descriptografado.

Levando em consideração os relatórios de avaliação do TPS, os investigadores conseguiram alterar dados do BU, que foi detectado pelos mecanismos de segurança da urna que não fizeram a assinatura do mesmo, fazendo com que a integridade do sistema não fosse quebrada. Outros investigadores conseguiram acessar o RDV e recuperar a ordem de votação, mas como não foi possível ter acesso a ordem dos eleitores, o sigilo do voto foi mantido. Dessa forma pode-se observar uma semelhança entre os dois sistemas, tendo em vista que os dois preservaram os dados dos eleitores.

O *STAR-Vote*, sistema descrito em Pereira e Wallach (2017), é semelhante ao sistema eleitoral brasileiro, visto que os dois possuem uma grande variedade de mecanismos de segurança capazes de detectar fraudes e adulterações.

O modelo apresentado por Babenko, Pisarev e Makarevich (2017) também se mostra semelhante ao sistema utilizado no Brasil, mesmo utilizando-se de outro tipo de criptografia apresenta os mesmos resultados quanto a segurança do sistema, levando em conta a criação do mesmo, com objetivos de eliminar a intervenção humana no processo de totalização de resultados e impedir que qualquer pessoa possa votar sem que esteja devidamente autenticada.

Por fim, o sistema eleitoral brasileiro tem se mostrado muito a frente do sistema apresentado no estudo de Lavanya (2011), levando em consideração que os testes realizados com a urna eletrônica brasileira não permitiu que os investigadores conseguissem ter sucesso absoluto nos ataques ao sistema sem que deixasse algum tipo de rastro que pudesse ser detectado.

6.4 CONSIDERAÇÕES FINAIS

Países como a Índia, Federação Russa e alguns estados dos Estados Unidos da América são exemplos de democracias que fazem uso de sistemas supervisionados, semelhantes ao sistema utilizado no Brasil. Dessa forma, o sistema brasileiro foi comparado aos sistemas desses países com o objetivo de apontar semelhanças e diferenças na implementação dos mesmos.

A análise desses sistemas mostra que o sistema eletrônico eleitoral do Brasil está em vantagem sob os sistemas utilizados por esses países, visto que muitos problemas enfrentados por eles, não são enfrentados no Brasil. É importante ressaltar que esse comparativo foi feito considerando os resultados obtidos pelo MS presente no Capítulo **??**.

7 CONCLUSÃO

A transparência do processo eleitoral vem sendo implementada a vários anos através do sistema informatizado, visto que a votação com cédulas de papel era um processo muito propenso a falhas. A modernização começou quando alguns inventores desenvolveram protótipos de urnas com intuito de agilizar o processo eleitoral, objetivando maior segurança e transparência. Várias ideias e protótipos de máquinas de votar surgiram até a primeira urna eletrônica ser de fato produzida e o voto se tornar eletrônico, o que aconteceu em 1996.

A informatização do voto ganhou forma quando a Justiça Eleitoral iniciou o recadastramento do eleitorado e seguiu-se com a criação da primeira urna eletrônica. Depois da primeira seção totalmente informatizada, as urnas foram distribuídas para as seções eleitorais do país inteiro. Tendo em vista que o sistema de autenticação dos eleitores ainda era complexo, a Justiça Eleitoral novamente deu início ao processo de melhoria do sistema, trazendo a identificação e autenticação biométrica, o qual vem sendo implantada com sucesso desde 2008.

No ano de 2009, a Justiça Eleitoral tomou uma importante iniciativa para o aprimoramento do sistema eletrônico utilizado no Brasil, através da criação dos Testes Públicos de Segurança, o qual, consiste num evento que reúne diversos especialistas das áreas de segurança e eletrônica do país que têm total liberdade para executar planos de ataque contra a urna eletrônica vigente. O seu objetivo principal é testar a segurança, integridade e autenticidade da mesma a fim de revelar vulnerabilidades que serão prontamente corrigidas, além de avaliar a confiabilidade do processo e a segurança do voto sigiloso.

Um sistema de votação seguro é garantia de coerção do eleitor e livre exercício da sua cidadania, visto que ninguém poderá saber em quem de fato ele votou. Com a realização das edições do TPS, foi possível observar que, cada vez mais, esse direito vem sendo garantido ao eleitor, visto que, nem mesmo com o relaxamento das medidas de segurança da urna para facilitar a execução dos planos de ataque, fora possível relacionar

um voto a um eleitor.

Em edições passadas do TPS, vulnerabilidades como a possibilidade da escuta da radiação eletromagnética ou das instruções de áudio da urna foram detectadas pelos especialistas durante os testes. Em um cenário real, um atacante teria muitas barreiras físicas para enfrentar até que conseguisse roubar informações executando este tipo de ataque. Porém, de todo modo, o TSE adicionou camadas de segurança ao processo para corrigir tais vulnerabilidades, demonstrando o esforço em não dispor de brechas atacáveis no sistema.

Toda edição do TPS visa trazer novos tópicos que cubram cada vez mais a descoberta de possíveis vulnerabilidades tecnológicas do sistema eleitoral brasileiro. A 5ª edição do evento, a ser realizada no ano de 2019, trará novidades quanto a de execução de planos de ataque. Na referida edição, também estará a disposição dos investigadores, o sistema de transmissão de votos, que trata de como é realizada a logística de centralização de informações entre todas as urnas eleitorais do país no processo de apuração dos votos, o qual não era alvo dos planos de ataques nas edições anteriores. Outro tema que poderá ser abordado em edições futuras do TPS, é a biometria do sistema eleitoral, que ainda não se encontra nos temas explorados pelo evento. Porém, o mesmo já foi sugerido ao TSE por investigadores das edições passadas à inclusão ao TPS.

Destaca-se, principalmente, a evolução tecnológica do Brasil, visto o destaque obtido na sociedade ao inserir essa tecnologia no processo eleitoral. Essa técnica também vem sendo implantada em diversos países do mundo, que também mostraram-se preocupados em utilizar meios eletrônicos para a modernização do vosso processo eleitoral. Ressalta-se que muitos países possuem um sistema semelhante ao utilizado pelo Brasil. Destes sistemas, muitos mostraram a presença de falhas, das quais não foram detectadas no sistema brasileiro. Outros, porém, possuem mecanismos de segurança tão seguros quanto aos do sistema brasileiro. Dessa forma, pode-se concluir que o eleitor brasileiro está seguro quanto ao sigilo do seu voto e a segurança do processo eleitoral no qual participa.

7.1 CONTRIBUIÇÕES DO TRABALHO

Levando em consideração os objetivos definidos na Seção 1.2, é possível afirmar que os mesmos foram alcançados durante a realização deste trabalho. Tal feito fora comprovado através dos resultados alcançados pelo MS, que mapeou as características de sistemas eletrônicos de votação utilizados em diversos países do mundo, e pelo estudo de

caso, que elencou as principais vulnerabilidades encontradas no sistema eleitoral brasileiro.

Nesse sentido, por meio do estudo de caso pode-se observar que, mesmo nos ataques que foram bem executados e alcançaram bons resultados, a anonimidade do voto foi preservada, uma vez que foi impossível relacioná-lo ao nome do eleitor. Da mesma forma, é possível provar a confidencialidade do processo, uma vez que os resultados da eleição não foram expostos a entidades mal intencionadas e sim somente à parte interessada, no caso o TSE.

A integridade de uma eleição consiste em o eleitor saber que o sistema que ele está utilizando é original do TSE, tanto quanto o TSE saber que o voto do eleitor não sofreu alterações. Sendo assim, o TSE disponibiliza a listas dos *hashes* dos programas utilizados pela urna para que, em qualquer lugar do Brasil, seja possível fazer a comparação do *hash* do programa utilizado pela urna com a lista disponibilizada pelo TSE, como forma de verificar autenticidade do mesmo. Por outro lado, o TSE utiliza mecanismos de segurança próprios para comprovar a integridade dos dos dados eleitorais, garantindo que os votos dos eleitores não tenham sofrido adulterações.

Os resultados obtidos apontam um grande número de tentativas de modificações nos sistemas utilizados pela urna. Essas tentativas, quando realizadas, foram rapidamente detectadas, impossibilitando que uma urna com funcionamento malicioso fosse utilizada em uma eleição. Além disso, o TSE buscar manter o aprimoramento constante da urna eletrônica brasileira, de modo que a segurança da mesma seja reforçada.

A iniciativa do recadastramento biométrico como forma de autenticação dos eleitores, implantado a partir de 2008 pela Justiça Eleitoral, vem atingindo seus objetivos de efetividade e abrangência territorial. Tal medida garante aos eleitores o direito à democracia, visto que o sistema em questão impede que um eleitor se passe por outro e vote em seu lugar. Esse processo implementa a técnica SYA (*Somethime You Are*), que se baseia no discernimento de características físicas do usuário. Por ser uma técnica robusta, ela tem o objetivo de aumentar a confiabilidade do processo.

7.2 TRABALHOS FUTUROS

Como trabalhos futuros, sugere-se complementar o estudo de caso realizado neste trabalho com as informações do TPS realizado no ano de 2019. Isso porque, novos planos de ataque serão realizados contra o sistema eletrônico, podendo ou não resultar em novas vulnerabilidades. Além disso, a referida edição do evento passará a abordar também o

processo de transmissão dos votos, onde um novo leque de possíveis vulnerabilidades serão exploradas pelos especialistas, a fim de aprimorar ainda mais a segurança do sistema vigente.

Outra sugestão, é complementar o mapeamento sistemático por meio de Busca Manual e *Snowballing* para verificar a existência de possíveis estudos que possam contribuir com a pesquisa. Essas buscas podem ser feitas através da análise de estudos publicados em eventos da área e também pela análise das referências dos estudos incluídos anteriormente.

REFERÊNCIAS

ABOSAMRA, K. M. et al. A practical, secure, and auditable e-voting system. **Journal of Information Security and Applications**, Elsevier, 2017.

ADAMEK, C. V. von et al. Sistema Eletrônico de Votação, Perguntas frequentes. p. 37, 2016.

ALVIM, F. F. Integridade eleitoral: significado e critérios de qualificação. **Revista Ballot**, v. 1, n. 2, p. 213–228, 2015.

ARANHA, D. F.; NUNES, T.; CARDOSO, C. Execução de código arbitrário na urna eletrônica brasileira. n. July, p. 1–36, 2018.

ARANHA, D. F.; RIBEIRO, H.; PARAENSE, A. L. O. Crowdsourced integrity verification of election results: An experience from Brazilian elections. **Annales des Telecommunications/Annals of Telecommunications**, v. 71, n. 7-8, p. 287–297, 2016. ISSN 19589395.

BABENKO, L.; PISAREV, I. Cryptographic protocol security verification of the electronic voting system based on blinded intermediaries. In: SPRINGER. **Proc. of the 3rd IITI**. [S.l.], 2018.

BABENKO, L.; PISAREV, I.; MAKAREVICH, O. A model of a secure electronic voting system based on blind intermediaries using russian cryptographic algorithms. In: ACM. **Proc. of the 10th SINCONF**. [S.l.], 2017.

BERNARDINETTI, S. Ex-juiz eleitoral escreve artigo sobre as urnas eletrônicas. **Tribunal Reginal Erelitoral do Paraná**, p. 1, 2018. Disponível em: <http://www.tre-pr.jus.br-/imprensa/noticias-tre-pr/2018/Junho/ex-juiz-escreve-artigo- sobre-as-urnas-eletronicas>.

BISTARELLI, S. et al. End-to-end voting with non-permissioned and permissioned ledgers. **Journal of Grid Computing**, Springer, 2019.

BRERETON, P. et al. Lessons from applying the systematic literature review process within the software engineering domain. **Systems and Software**, New York, USA, v. 80, p. 571–583, 2007.

CABRAL, J. C. d. R. **Código Eleitoral da República dos Estados Unidos do Brasil (1932)**. 2004. 1–215 p.

CHANG, D. et al. Apollo: End-to-end verifiable voting protocol using mixnet and hidden tweaks. In: SPRINGER. **Proc. of the 18th ICISC**. [S.l.], 2015.

Confederação Nacional das Instituições Financeiras. **Brasil adere ao Instituto Internacional para a Democracia e a Assistência Eleitoral**. 2016. Disponível em: <https://cnf.org.br/brasil-adere-ao-instituto-internacional-para-a-democracia-e-a-assistencia-eleitoral/>. Acesso em: 17/11/2019.

CORTIER, V.; SMYTH, B. Attacking and fixing helios: An analysis of ballot secrecy. **Journal of Computer Security**, IOS Press, 2013.

DANTAS, M. L. **Uma Abordagem Focada em Gestão de Riscos**. [S.l.: s.n.], 2011. 147 p. ISBN 9788540600478.

DOSSOGNE, J.; LAFITTE, F. Blinded additively homomorphic encryption schemes for self-tallying voting. **Journal of Information Security and Applications**, Elsevier, 2015.

EASTERBROOK, S. et al. Selecting empirical methods for software engineering research. In: **Guide to advanced empirical software engineering**. [S.l.]: Springer, 2008. p. 285–311.

FAGUNDES, E. M. **Segurança da Informação**. 2018. Disponível em: <http://efagundes-.com/artigos/seguranca-da-informacao/>. Acesso em: 2018-11-05.

FALBO, R. D. A. Mapeamento Sistemático. n. 2010, 2013.

FREITAS, W. R.; JABBOUR, C. J. C. Utilizando estudo de caso(s) como estratégia de pesquisa qualitativa: Boas práticas e sugestões. **Estudo & Debate**, Lajeado, v. 18, 2011.

FUCK, L. F. et al. Urna eletrônica, 20 anos a favor da democracia. p. 43, 2016.

GURUBASAVANNA, M. et al. Multimode authentication based electronic voting kiosk using raspberry pi. In: IEEE. **Proc. of the 2nd International Conference on I-SMAC**. [S.l.], 2018.

HAINES, T.; BOYEN, X. Truly multi-authority 'prêt-à-voter'. In: SPRINGER. **Proc. of the E-Vote-ID**. [S.l.], 2016.

HEIDERICH, M. et al. The bug that made me president a browser-and web-security case study on helios voting. In: SPRINGER. **Proc. of the 3rd Vote-ID**. [S.l.], 2011.

HSIAO, T.-C. et al. Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme. **Advances in Mechanical Engineering**, SAGE Publications Sage UK: London, England, 2017.

HUARTE, M. et al. A new fully auditable proposal for an internet voting system with secure individual verification and complaining capabilities. In: IEEE. **Proc. of the 10th SECRYPT**. [S.l.], 2013.

HUSSIEN, H.; ABOELNAGA, H. Design of a secured e-voting system. In: IEEE. **Proc. of the ICCAT**. [S.l.], 2013.

International Institute for Democracy and Electoral Assistance. **Use of E-Voting Around the World**. 2015. Disponível em: <https://www.idea.int/news-media/media/use-e-voting-around-world>. Acesso em: 17/11/2019.

JIN, C. et al. Heterogeneous deniable authentication and its application to e-voting systems. **Journal of Information Security and Applications**, Elsevier, 2019.

Justiça Eleitoral. **Teste Público de Segurança 2019**. 2019. Disponível em: <http:/-/www.justicaeleitoral.jus.br/tps/>. Acesso em: 31/10/2019.

KARTIT, Z. et al. Towards a secure electronic voting in cloud computing environment using homomorphic encryption algorithm. **International Journal of Applied Engineering Research**, 2015.

KATE, N.; KATTI, J. Security of remote voting system based on visual cryptography and sha. In: IEEE. **Proc. of the ICCUBEA**. [S.l.], 2016.

KHELIFI, A. et al. M-vote: a reliable and highly secure mobile voting system. In: IEEE. **Proc. of the PICICT**. [S.l.], 2013.

KIAYIAS, A.; ZACHARIAS, T.; ZHANG, B. On the necessity of auditing for election privacy in e-voting systems. In: SPRINGER. **Proc. of the e-Democracy**. [S.l.], 2015.

KIAYIAS, A.; ZACHARIAS, T.; ZHANG, B. Auditing for privacy in threshold pke e-voting. **Information & Computer Security**, Emerald Publishing Limited, 2017.

KIM, C. S. et al. A study on the ubiquitous e-voting system for the implementation of e-government. **International Journal of Security & Its Applications**, 2013.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering – a systematic literature review. **Information and Software Technology**, v. 51, p. 7–15, 2009.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering–a tertiary study. **Information and Software Technology**, Elsevier, 2010.

KUMAR, M.; KATTI, C. P.; SAXENA, P. C. A secure anonymous e-voting system using identity-based blind signature scheme. In: SPRINGER. **Proc. of the ICISSP**. [S.l.], 2017.

LAKSHMI, C. J.; KALPANA, S. Secured and transparent voting system using biometrics. In: IEEE. **Proc. of the 2nd ICISC**. [S.l.], 2018.

LAVANYA, S. Trusted secure electronic voting machine. In: IEEE. **Proc. of the ICONSET**. [S.l.], 2011.

LEE, K. et al. Protection profile for secure e-voting systems. In: SPRINGER. **Proc. of the 6th ISPEC**. [S.l.], 2010.

LYRA, M. R. **Governança da Segurança da Informação**. [S.l.: s.n.], 2015. 160p p. ISBN 9788592026417.

MARCIANO, J. L. P. **Segurança da Informação - uma abordagem social**. 2006. 211 p.

MAZIERO, C. A. Sistemas Operacionais: Conceitos e Mecanismos. p. 356, 2017.

MOHAMMADPOURFARD, M. et al. A new secure internet voting protocol using java card 3 technology and java information flow concept. **Security and Communication Networks**, Wiley Online Library, 2015.

MONTEIRO, J. et al. Protegendo o sistema operacional e chaves criptográaficas numa urna eletrônica do tipo t-dre. In: **SBSeg 2019 - WTE ()**. [S.l.: s.n.], 2019.

NASSAR, M.; MALLUHI, Q.; KHAN, T. A scheme for three-way secure and verifiable e-voting. In: IEEE. **Proc. of the 15th AICCSA**. [S.l.], 2018.

NBR ISSO/IEC 17799:2005. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**, p. 120, 2005.

NGUYEN, T. A. T.; DANG, T. K. Enhanced security in internet voting protocol using blind signature and dynamic ballots. **Electronic Commerce Research**, Springer, 2013.

NGUYEN, T. A. T.; DANG, T. K. A practical solution against corrupted parties and coercers in electronic voting protocol over the network. In: SPRINGER. **Proc. of the ICT-EurAsia**. [S.l.], 2013.

OLEMBO, M. M.; SCHMIDT, P.; VOLKAMER, M. Introducing verifiability in the polyas remote electronic voting system. In: IEEE. **Proc. of the 6th ARES**. [S.l.], 2011.

Olhar Digital. **Como funcionam as urnas eletrônicas de outros países**. 2018. Disponível em: <https://olhardigital.com.br/noticia/como-funcionam-as-urnas-eletronicas-de-outros-paises/78982l>. Acesso em: 17/11/2019.

PEGORINI, J. et al. Desafios e soluções em sistemas de votação eletrônica: Um mapeamento sistemático. In: **SBSeg 2019 - WTE ()**. [S.l.: s.n.], 2019.

PENG, K. A general and efficient countermeasure to relation attacks in mix-based e-voting. **International Journal of Information Security**, Springer, 2011.

PEREIRA, O.; WALLACH, D. S. Clash attacks and the star-vote system. In: SPRINGER. **Proc. of the E-Vote-ID**. [S.l.], 2017.

RURA, L.; ISSAC, B.; HALDAR, M. Vulnerability studies of e2e voting systems. In: **Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering**. [S.l.]: Springer, 2015.

SAQIB, M. N. et al. Anonymous and formally verified dual signature based online e-voting protocol. **Cluster Computing**, Springer, 2018.

SEBÉ, F. et al. Simple and efficient hash-based verifiable mixing for remote electronic voting. **Computer Communications**, Elsevier, 2010.

SHAKIBA, N. M.; DOOSTARI, M.-A.; MOHAMMADPOURFARD, M. Esiv: an end-to-end secure internet voting system. **Electronic Commerce Research**, Springer, 2017.

SILVEIRA, C. M. Do voto em papel ao eletrônico: Um estudo de caso da implantação do voto biométrico em Canoas/RS. **Journal of Strategic Studies**, v. 34, n. 2, p. 281–293, 2011. ISSN 0140-2390.

SMARTMATIC. **Benefícios do voto eletrônico**. 2018. Disponível em: <http://www-.smartmatic.com/pt/votacao/voto-eletronico/>. Acesso em: 2018-10-14.

SPYCHER, O.; HAENNI, R. A novel protocol to allow revocation of votes a hybrid voting system. In: IEEE. **Proc. of the ISSA**. [S.l.], 2010.

SRINIVASAN, S. et al. Countering ballot stuffing and incorporating eligibility verifiability in helios. In: SPRINGER. **Proc. of the NSS**. [S.l.], 2013.

SYDON, S. T. **Delitos Informáticos Próprios : Uma Abordagem Sob a Perspectiva Vitimodogmática .** 2009. 282 p.

TAVARES, A. R. Estudos Eleitorais. **Tribunal Superior Eleitoral - SC**, v. 6, p. 130, 2011.

TORNOS, J. L.; SALAZAR, J. L.; PILES, J. J. Optimizing ring signature keys for e-voting. In: IEEE. **Proc. of the IWCMC**. [S.l.], 2015.

Tribunal Regional de Santa Catarina. **Histórico do TRE-SC**. 2015. Disponível em: <http://www.tre-sc.jus.br/site/institucional/memoria/historico-do-tresc/index-.html>. Acesso em: 04/11/2018.

Tribunal Superior Eleitora. **Votação eletrônica é realidade em mais de 30 países**. 2018. 1 p. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2018/Marco-/votacao-eletronica-e-realidade-em-mais-de-30-paises>. Acesso em: 15/10/2018.

Tribunal Superior Eleitoral. **Teste da equipe da UnB contribui para aprimoramento do sigilo do voto**. 2012. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse-/2012/Marco/teste-da-equipe-da-unb-reforca-sigilo-do-voto>. Acesso em: 14/11/2019.

Tribunal Superior Eleitoral. **Eleições Seguras: saiba como surgiu a urna eletrônica e por que ela está em constante processo de evolução**. 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Agosto/eleicoes-seguras-saiba-como-surgiu-a-urna-eletronica-e-por-que-ela-esta-em-constante-processo-de-evolucao>. Acesso em: 23/10/2018.

Tribunal Superior Eleitoral. **TSE celebra adesão do Brasil ao Instituto Internacional para a Democracia e Assistência Eleitoral**. 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Abril/tse-celebra-adesao-do-brasil-ao-instituto-internacional-para-a-democracia-e-assistencia-eleitoral>. Acesso em: 17/11/2019.

Tribunal Superior Eleitoral. **Criptografia**. 2019. Disponível em: <http://www.tse.jus.br-/eleicoes/urna-eletronica/seguranca-da-urna/criptografia>. Acesso em: 17/11/2019.

Tribunal Superior Eleitoral. **Teste Público de Segurança**. 2019. Disponível em: <http:-//www.tse.jus.br/eleicoes/urna-eletronica/seguranca>. Acesso em: 31/10/2019.

Uol - Folha de São Paulo. **Tradicional tinta azul antifraude é símbolo das eleições na Índia**. 2018. Disponível em: <https://www1.folha.uol.com.br/mundo/2019-/04/tradicional-tinta-azul-antifraude-e-simbolo-das-eleicoes-na-india.shtml>. Acesso em: 17/11/2019.

WILL, M. A. et al. Secure voting in the cloud using homomorphic encryption and mobile agents. In: IEEE. **Proc. of the ICCCRI**. [S.l.], 2015.

WOHLIN, C.; AURUM, A. Towards a decision-making structure for selecting a research design in empirical software engineering. **Empirical Software Engineering**, Springer, v. 20, n. 6, p. 1427–1455, 2015.

WOHLIN, C. et al. **Experimentation in Software Engineering**. [S.l.]: Springer, 2012. 1427–1455 p.

YOON, E.-J. et al. Robust deniable authentication protocol. **Wireless Personal Communications**, Springer, 2010.

YU, B. et al. Platform-independent secure blockchain-based voting system. In: SPRINGER. **Proc. of the ISC**. [S.l.], 2018.

ZHANG, H.; YOU, Q.; ZHANG, J. A lightweight electronic voting scheme based on blind signature and kerberos mechanism. In: IEEE. **Proc. of the 5th ICEIEC**. [S.l.], 2015.

ZHOU, Y. et al. Mvp: an efficient anonymous e-voting protocol. In: IEEE. **Proc. of the GLOBECOM**. [S.l.], 2016.

ZHU, Y.; ZENG, Z.; LV, C. Anonymous voting scheme for boardroom with blockchain. **International Journal of Performability Engineering**, 2018.

ZISSIS, D.; LEKKAS, D. Securing e-government and e-voting with an open cloud computing architecture. **Government Information Quarterly**, v. 28, n. 2, p. 239 – 251, 2011. ISSN 0740-624X.